

**JP2002374240A**

**RECEPTION TERMINAL, KEY APPARATUS, AND KEY UPDATING METHOD FOR PUBLIC KEY CRYPTOSYSTEM**

Publication number : JP2002374240A

Date of publication of application : 26.12.2002

Application number : 2002-109744

Applicant : MATSUSHITA ELECTRIC IND CO LTD

Date of filing : 11.04.2002

Inventor : YOKOTA KAORU

TATEBAYASHI MAKOTO

Priority

Priority number : 2001113667    Priority date : 12.04.2001    Priority country : JP

Abstract:

PROBLEM TO BE SOLVED: To provide a method for enabling a distribution side or a key management center to take the initiative in updating of the keys.

SOLUTION: The distribution system 100 includes a secret key managing unit 132, that secretly receives an update secret key; a public key managing unit 111 that receives an update public key; a distribution key generating unit 112 that generates the update public key and the distribution secret key; an encryption unit 113 that encrypts the distribution secret key, by using the update public key to generate an encrypted secret key; a transmission unit 114 that transmits the encrypted secret key; a public key updating unit 115 that updates the distribution public key used for data distribution into the generated distribution public key, after the transmission section 114 has transmitted the encrypted secret key; a secret key receiving unit 137 that receives the encrypted secret key; and a secret key updating unit 138 that updates the distribution secret key used for data distribution into the distribution secret key decrypted by using the update secret key to decrypt the encrypted secret key, as required, after the encrypted secret key is received.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-374240  
(P2002-374240A)

(43) 公開日 平成14年12月26日 (2002. 12. 26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テームコード* (参考)
H 0 4 L 9/08		G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 K 17/00	L 5 B 0 5 8
G 0 6 K 17/00		H 0 4 L 9/00	6 0 1 B 5 J 1 0 4
H 0 4 L 9/10			6 0 1 F
			6 2 1 A

審査請求 未請求 請求項の数20 O L (全 22 頁)

(21) 出願番号 特願2002-109744(P2002-109744)  
(22) 出願日 平成14年4月11日 (2002. 4. 11)  
(31) 優先権主張番号 特願2001-113667(P2001-113667)  
(32) 優先日 平成13年4月12日 (2001. 4. 12)  
(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821  
松下電器産業株式会社  
大阪府門真市大字門真1006番地  
(72) 発明者 横田 薫  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(72) 発明者 館林 誠  
大阪府門真市大字門真1006番地 松下電器  
産業株式会社内  
(74) 代理人 100090446  
弁理士 中島 司朗

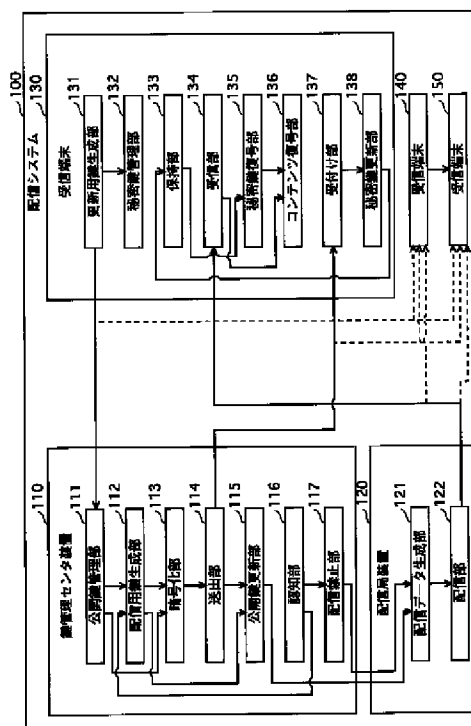
最終頁に続く

(54) 【発明の名称】 公開鍵暗号方式の鍵の更新方法、受信端末及び鍵管理装置

(57) 【要約】

【課題】 配信側や鍵管理センタが鍵更新の主導権を持つことができるデータ配信システムを提供する。

【解決手段】 更新用秘密鍵を入手する秘密鍵管理部132、更新用公開鍵を入手する公開鍵管理部111、配信用公開鍵と配信用秘密鍵とを生成する配信用鍵生成部112、配信用秘密鍵を更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成する暗号化部113、暗号化秘密鍵を送出する送出部114、暗号化秘密鍵が送出された後は、データ配信の際に使用される配信用公開鍵を、生成された配信用公開鍵に更新する公開鍵更新部115、暗号化秘密鍵を受付ける受け付け部137、及び、暗号化秘密鍵が受け付けられた後は、データ配信の際に使用される配信用秘密鍵を、更新用秘密鍵を用いて暗号化秘密鍵を必要に応じて復号することにより復元される配信用秘密鍵に更新する秘密鍵更新部138を備える。



【特許請求の範囲】

【請求項1】 鍵管理センタと、配信局と、1つ以上の受信端末とを含むデータ配信システムにおいて、公開鍵暗号方式の鍵ペアをなす配信用公開鍵及び配信用秘密鍵を更新する更新方法であって、配信用公開鍵は、配信すべきデータを暗号化して暗号化データを生成する際に用いられ、配信用秘密鍵は、配信された暗号化データを復号する際に用いられ、当該更新方法は、所定の受信端末において、データ配信を始める前に、更新用秘密鍵を入手する秘密鍵入手ステップと、前記鍵管理センタにおいて、データ配信を始める前に、前記更新用秘密鍵と鍵ペアをなす更新用公開鍵を入手する公開鍵入手ステップと、前記鍵管理センタにおいて、前記受信端末用に、配信用公開鍵、及び、配信用秘密鍵を生成する生成ステップと、前記鍵管理センタにおいて、前記生成ステップにより生成された配信用秘密鍵を、前記公開鍵入手ステップにより入手された更新用公開鍵を用いて暗号化して、暗号化秘密鍵を生成する暗号化ステップと、前記鍵管理センタにおいて、任意のタイミングで、前記暗号化ステップにより生成された暗号化秘密鍵を、前記受信端末へ向けて送出する送出ステップと、前記鍵管理センタにおいて、前記送出ステップにより暗号化秘密鍵が前記受信端末へ向けて送出された後は、データ配信の際に配信局により使用される当該受信端末用の配信用公開鍵を、それまで使用されていた配信用公開鍵から、前記生成手段により当該受信端末用に生成された配信用公開鍵に更新する公開鍵更新ステップと、前記受信端末において、前記送出ステップにより送出された暗号化秘密鍵を受付ける受け付けステップと、前記受信端末において、前記受け付けステップにより暗号化秘密鍵が受け付けられた後は、当該受信端末用の配信用秘密鍵を、それまで使用していた配信用秘密鍵から、前記秘密鍵入手ステップにより入手された更新用秘密鍵を用いて当該暗号化秘密鍵を必要に応じて復号することにより復元される配信用秘密鍵に更新する秘密鍵更新ステップとを含むことを特徴とする更新方法。

【請求項2】 前記暗号化ステップは、さらに、生成する暗号化秘密鍵に、当該暗号化秘密鍵の正当性を示すデジタル署名を施し、前記秘密鍵更新ステップは、前記受け付けステップにより受け付けられた暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が正当なものであるか否かを判断し、正当なものであると判断した場合に配信用秘密鍵を更新し、正当なものではないと判断した場合に配信用秘密鍵を更新しないことを特徴とする請求項1に記載の更新方法。

【請求項3】 前記受信端末は複数であり、

それぞれの受信端末用の配信用公開鍵は、配信すべきデータをそれぞれ暗号化して暗号化データを生成する際に用いられ、それぞれの受信端末用の配信用秘密鍵は、対応する受信端末において、配信された暗号化データを復号する際に用いられ、前記秘密鍵入手ステップは、それぞれの受信端末において、それぞれユニークな更新用秘密鍵を入手し、前記公開鍵入手ステップは、前記鍵管理センタにおいて、それぞれの受信端末用のそれぞれユニークな更新用公開鍵を入手し、前記生成ステップは、前記鍵管理センタにおいて、それぞれの受信端末用に、それぞれユニークな配信用公開鍵、及び、配信用秘密鍵を生成し、前記暗号化ステップは、前記鍵管理センタにおいて、前記生成ステップによりそれぞれの受信端末用に生成された配信用秘密鍵を、それぞれの受信端末用の更新用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化秘密鍵を生成し、前記送出ステップは、前記鍵管理センタにおいて、任意のタイミングで一斉に、前記暗号化ステップにより生成されたそれぞれの受信端末用の暗号化秘密鍵を、それぞれの受信端末へ向けて送出し、前記公開鍵更新ステップは、前記鍵管理センタにおいて、前記送出ステップによりそれぞれの受信端末用の暗号化秘密鍵がそれぞれの受信端末へ向けて、一斉に送出された後は、データ配信の際に配信局により使用されるそれぞれの受信端末用の配信用公開鍵を、それまで使用されていた配信用公開鍵から、前記生成ステップによりそれぞれの受信端末用に生成された配信用公開鍵に更新し、前記受け付けステップは、それぞれの受信端末において、前記送出ステップにより送出されたそれぞれの受信端末用の暗号化秘密鍵を受け付け、前記秘密鍵更新ステップは、それぞれの受信端末において、前記受け付けステップによりそれぞれの受信端末用の暗号化秘密鍵が受け付けられた後は、それぞれの受信端末用の配信用秘密鍵を、それまで使用していた配信用秘密鍵から、秘密鍵入手ステップにより入手されたそれぞれの更新用秘密鍵を用いて当該暗号化秘密鍵を必要に応じて復号することにより復元される配信用秘密鍵に更新することを特徴とする請求項1に記載の更新方法。

【請求項4】 当該更新方法は、さらに、前記配信局において、データ配信を中止すべき受信端末を認知する認知ステップと、

前記配信局において、前記認知ステップによりデータ配信を中止すべき受信端末が認知された以後は、当該受信端末用の暗号化データの配信を禁止する配信禁止ステップとを含むことを特徴とする請求項3に記載の更新方法。

【請求項5】 当該更新方法は、さらに、前記鍵管理センタにおいて、配信用秘密鍵を更新すべき受信端末を認知する認知ステップを含み、前記生成ステップは、前記鍵管理センタにおいて、前記認知ステップにより認知された受信端末用の配信用公開鍵、及び、配信用秘密鍵を生成し、前記暗号化ステップは、前記鍵管理センタにおいて、前記認知ステップにより認知された受信端末用に、前記生成ステップにより生成された配信用秘密鍵を、当該受信端末用の更新用公開鍵を用いて暗号化して、当該受信端末用の暗号化秘密鍵を生成し、前記送出ステップは、前記鍵管理センタにおいて、前記認知ステップにより認知された受信端末用に、前記暗号化ステップにより生成された暗号化秘密鍵を、当該受信端末へ向けて送出し、前記公開鍵更新ステップは、前記鍵管理センタにおいて、前記認知ステップにより認知された受信端末へ向けて、暗号化秘密鍵が送出された後は、データ配信の際に配信局により使用される当該受信端末用の配信用公開鍵を、それまで使用されていた配信用公開鍵から、前記生成ステップにより当該受信端末用に生成された配信用公開鍵に更新し、前記秘密鍵更新ステップは、前記認知ステップにより認知された受信端末において、当該受信端末用の暗号化秘密鍵が受け付けられた後は、当該受信端末用の配信用秘密鍵を、それまで使用していた配信用秘密鍵から、秘密鍵入手ステップにより入手された更新用秘密鍵を用いて必要に応じて復号することにより復元される配信用秘密鍵に更新することを特徴とする請求項3に記載の更新方法。

【請求項6】 それぞれの受信端末用の配信用公開鍵を用いてそれぞれ暗号化される配信すべきデータは、秘密鍵暗号方式の鍵であるコンテンツ鍵であり、前記配信局は、それぞれの受信端末用の配信用公開鍵を用いて、前記コンテンツ鍵を暗号化して、それぞれの受信端末用の暗号化コンテンツ鍵を生成し、配信すべきコンテンツを、前記コンテンツ鍵を用いて暗号化して暗号化コンテンツを生成し、前記それぞれの受信端末用の暗号化コンテンツ鍵の全てと、前記暗号化コンテンツとを、全ての受信端末へ配信し、前記それぞれの受信端末は、前記配信局より配信された全ての暗号化コンテンツ鍵と暗号化コンテンツとを受信し、当該受信端末用の暗号化コンテンツ鍵を、当該受信

端末用の配信用秘密鍵を用いて復号して前記コンテンツ鍵を復元し、前記暗号化コンテンツを、当該コンテンツ鍵を用いて復号してコンテンツを復元することとを特徴とする請求項3に記載の更新方法。

【請求項7】 前記受信端末は、当該受信端末用の暗号化秘密鍵を記録したＩＣカードを備え、当該暗号化秘密鍵を復号して配信用秘密鍵を生成し、受信した暗号化データを、当該配信用秘密鍵を用いて復号し、前記送出ステップは、前記鍵管理センタにおいて、前記暗号化ステップにより生成された前記受信端末用の暗号化秘密鍵を、新しいＩＣカードに記録して、当該受信端末へ向けて送出し、前記受け付けステップは、前記受信端末において、前記新しいＩＣカードを受け付け、前記秘密鍵更新ステップは、前記受信端末において、前記新しいＩＣカードが受け付けられた後に、元々備えていたＩＣカードが、当該新しいＩＣカードと差し換えられることにより、配信用秘密鍵が更新されることを特徴とする請求項1に記載の更新方法。

【請求項8】 所定データが当該受信端末用の配信用公開鍵を用いて暗号化されることにより生成された、配信局から配信される暗号化データを受信して、当該暗号化データを、当該受信端末用の配信用秘密鍵を用いて復号して、前記所定データを得る受信端末であって、データ配信を始める前に、更新用秘密鍵を入手する秘密鍵入手手段と、当該受信端末用の配信用秘密鍵が、前記更新用秘密鍵と鍵ペアをなす更新用公開鍵を用いて暗号化されることにより生成された暗号化秘密鍵を保持する保持手段と、前記配信局より配信される前記暗号化データを受信する受信手段と、前記保持手段に保持されている暗号化秘密鍵を、前記秘密鍵入手手段により入手された更新用秘密鍵を用いて復号して、当該受信端末用の配信用秘密鍵を復元する秘密鍵復号手段と、前記受信手段により受信された暗号化データを、前記秘密鍵復号手段により復元された配信用秘密鍵を用いて復号して、前記所定データを得るデータ復号手段とを備えることを特徴とする受信端末。

【請求項9】 当該受信端末は、さらに、鍵管理センタから任意のタイミングで送出される暗号化秘密鍵を受け付ける受け付け手段を備え、前記暗号化秘密鍵は、前記鍵管理センタにおいて、当該受信端末用に、公開鍵暗号方式の鍵ペアをなす配信用公開鍵、及び、配信用秘密鍵が生成され、前記更新用公開鍵を用いて、当該配信用秘密鍵が暗号化されて生成され、当該受信端末は、さらに、

前記受付け手段により暗号化秘密鍵が受付けられた後は、前記保持手段に保持された暗号化秘密鍵を、当該受付けられた暗号化秘密鍵に更新する秘密鍵更新手段を備えることを特徴とする請求項 8 に記載の受信端末。

【請求項 10】 前記受付け手段により受け付けられる暗号化秘密鍵には、当該暗号化秘密鍵の正当性を示すデジタル署名が施されており、前記秘密鍵復号手段は、前記秘密鍵更新手段により暗号化秘密鍵が更新された後は、更新された暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が正当なものであるか否かを判断し、正当なものであると判断した場合に当該受信端末用の配信用秘密鍵を復元し、正当なものではないと判断した場合に当該受信端末用の配信用秘密鍵を復元しないことを特徴とする請求項 9 に記載の受信端末。

【請求項 11】 前記所定データは、秘密鍵暗号方式の鍵であるコンテンツ鍵であり、前記受信手段は、前記配信用公開鍵を用いて前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵と共に、当該コンテンツ鍵を用いて配信すべきコンテンツを暗号化して生成された暗号化コンテンツを受信し、前記データ復号手段は、前記受信手段により受信された暗号化コンテンツ鍵を、前記秘密鍵復号手段により復元された配信用秘密鍵を用いて復号して、前記コンテンツ鍵を得て、前記受信手段により受信された暗号化コンテンツを、当該コンテンツ鍵を用いて復号してコンテンツを得ることを特徴とする請求項 9 に記載の受信端末。

【請求項 12】 前記保持手段は、IC カードであり、前記受付け手段は、前記暗号化秘密鍵が記録された新しい IC カードを受け付け、前記秘密鍵更新手段は、前記新しい IC カードが受け付けられた後は、元々備えていた IC カードが、当該新しい IC カードと差し換えられることにより、配信用秘密鍵が更新されることを特徴とする請求項 9 に記載の受信端末。

【請求項 13】 データ配信を始める前に、更新用秘密鍵を保持している所定の受信端末用に、当該更新用秘密鍵と鍵ペアをなす更新用公開鍵を入手する公開鍵入手手段と、前記受信端末用に、公開鍵暗号方式の鍵ペアをなす配信用公開鍵、及び、配信用秘密鍵を生成する生成手段と、前記生成手段により生成された配信用秘密鍵を、前記公開鍵入手手段により入手された更新用公開鍵を用いて暗号化して、暗号化秘密鍵を生成する暗号化手段と、任意のタイミングで、前記暗号化手段により生成された暗号化秘密鍵を、前記受信端末へ向けて送出する送出手段と、

前記送出手段により暗号化秘密鍵が前記受信端末へ向けて送出された後は、データ配信の際に使用される当該受信端末用の配信用公開鍵を、それまで使用されていた配信用公開鍵から、前記生成手段により当該受信端末用に生成された配信用公開鍵に更新する公開鍵更新手段とを備えることを特徴とする鍵管理装置。

【請求項 14】 前記暗号化手段は、さらに、生成する暗号化秘密鍵に、当該暗号化秘密鍵の正当性を示すデジタル署名を施すことを特徴とする請求項 13 に記載の鍵管理装置。

【請求項 15】 前記公開鍵入手手段は、複数の受信端末用のそれぞれユニークな更新用公開鍵を入手し、前記生成手段は、それぞれの受信端末用に、それぞれユニークな配信用公開鍵、及び、配信用秘密鍵を生成し、前記暗号化手段は、前記生成手段によりそれぞれの受信端末用に生成された配信用秘密鍵を、それぞれの受信端末用の更新用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化秘密鍵を生成し、前記送出手段は、任意のタイミングで一斉に、前記暗号化手段により生成されたそれぞれの受信端末用の暗号化秘密鍵を、それぞれ対応する受信端末へ向けて送出し、前記公開鍵更新手段は、前記送出手段によりそれぞれの受信端末用の暗号化秘密鍵がそれぞれ対応する受信端末へ向けて、一斉に送出された後は、それぞれの受信端末用の配信用公開鍵を、それまで使用していた配信用公開鍵から、前記生成手段によりそれぞれの受信端末用に生成された配信用公開鍵に更新することを特徴とする請求項 13 に記載の鍵管理装置。

【請求項 16】 当該鍵管理装置は、さらに、データ配信を中止すべき受信端末を認知する認知手段と、前記認知手段によりデータ配信を中止すべき受信端末が認知された以後は、当該受信端末用の配信用公開鍵を用いたデータ配信を禁止する配信禁止手段とを備えることを特徴とする請求項 15 に記載の鍵管理装置。

【請求項 17】 当該鍵管理装置は、さらに、配信用秘密鍵を更新すべき受信端末を認知する認知手段を備え、前記生成手段は、前記認知手段により認知された受信端末用の配信用公開鍵、及び、配信用秘密鍵を生成し、前記暗号化手段は、前記認知手段により認知された受信端末用に、前記生成手段により生成された配信用秘密鍵を、当該受信端末用の更新用公開鍵を用いて暗号化して、当該受信端末用の暗号化秘密鍵を生成し、

前記送出手段は、  
前記認知手段により認知された受信端末用に、前記暗号化手段により生成された暗号化秘密鍵を、当該受信端末へ向けて送出し、

前記公開鍵更新手段は、  
前記認知手段により認知された受信端末へ向けて、暗号化秘密鍵が送出された後は、当該受信端末用の配信用公開鍵を、それまで使用されていた配信用公開鍵から、前記生成手段により当該受信端末用に生成された配信用公開鍵に更新することを特徴とする請求項 15 に記載の鍵管理装置。

【請求項 18】 当該鍵管理装置は、配信局と一体化しており、

当該鍵管理装置は、さらに、  
所定データを、それぞれの受信端末用の配信用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化データを生成する配信データ生成手段と、  
前記配信データ生成手段により生成されたそれぞれの受信端末用の暗号化データの全てを、全ての受信端末へ配信する配信手段とを備えることを特徴とする請求項 15 に記載の鍵管理装置。

【請求項 19】 前記所定データは、秘密鍵暗号方式の鍵であるコンテンツ鍵であり、

前記配信データ生成手段は、  
コンテンツ鍵を、それぞれの受信端末用の配信用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化コンテンツ鍵を生成すると共に、当該コンテンツ鍵を用いて配信すべきコンテンツを暗号化して暗号化コンテンツを生成し、

前記配信手段は、  
前記それぞれの受信端末用の暗号化コンテンツ鍵の全てと共に、前記配信データ生成手段により生成された前記暗号化コンテンツを、全ての受信端末へ配信することを特徴とする請求項 18 に記載の鍵管理装置。

【請求項 20】 前記受信端末は、当該受信端末用の暗号化秘密鍵を記録した IC カードを備え、データ配信の際に、当該暗号化秘密鍵を復号して配信用秘密鍵を生成して用い、

前記送出手段は、  
前記暗号化手段により生成された前記受信端末用の暗号化秘密鍵を、新しい IC カードに記録して、当該受信端末へ送ることを特徴とする請求項 13 に記載の鍵管理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、公開鍵暗号方式を用いたデータ配信システムにおける、鍵の更新方法に関する。

【0002】

【従来の技術】著作権のあるデジタルコンテンツ等のデ

ータが無断で使用されないように、デジタルコンテンツ等を暗号化して配信し、著作権料を支払う契約をしているような正当なユーザの装置のみに復号の為の復号鍵を付与しておく方法が考えられる（以下、暗号化されたデジタルコンテンツを「暗号化コンテンツ」と言う）。

【0003】このようにすると、正当なユーザの装置以外の他の装置では暗号化コンテンツを復号できないのでデジタルコンテンツの不正な使用を防ぐことができる。暗号方式には、秘密鍵暗号方式と公開鍵暗号方式とがある。これらの詳細は、池野信一、小山謙二著「現代暗号理論」（電子情報通信学会）に記載がある。秘密鍵暗号方式は、配信側と受信側とが同一の共通鍵を秘密に保持し、配信側が共通鍵を用いてデジタルコンテンツを暗号化し、受信側が共通鍵を用いてデジタルコンテンツに復号する。通常、配信側に対して受信側は複数存在するので、配信側では受信側の数だけ共通鍵を機密に管理しなければならず配信側の負担が大きい。

【0004】公開鍵暗号方式は、配信側が公開鍵を保持し、公開鍵を用いてデジタルコンテンツを暗号化し、受信側が秘密鍵を保持し、秘密鍵を用いてデジタルコンテンツを復号する。公開鍵は機密に管理する必要がないので、配信側の負担が小さい。また安全対策上、暗号化や復号に用いる鍵は定期的、或いは、必要に応じて更新することが望ましい。

【0005】秘密鍵暗号方式の共通鍵を更新するには、例えば受信側か配信側かのいずれか一方で新しい共通鍵を生成して、他方に新しい共通鍵を機密に伝達しなければならない。新しい共通鍵を第三者に知られてしまうと暗号化コンテンツが不正に使用されてしまうので、鍵伝達時の機密管理を徹底しなければならず、頻繁に鍵を更新する用途には向かない。

【0006】公開鍵暗号方式の公開鍵と秘密鍵とを更新するには、通常、受信側のそれぞれが公開鍵と秘密鍵との鍵ペアを生成して、公開鍵を配信側へ普通に送る。秘密鍵は伝達しないので、伝達時に第三者に知られる事はなく、公開鍵は第三者に知られても暗号化コンテンツが不正に使用される事はないので、鍵伝達時の機密管理が不要であり、頻繁に鍵を更新する用途に向いている。

【0007】以上のように、公開鍵暗号方式は、配信側が鍵を機密に管理する必要がない上に、鍵の更新が比較的簡単なので、著作権のあるデジタルコンテンツ等の配信システムに広く用いられている。

【0008】

【発明が解決しようとする課題】しかしながら、公開鍵暗号方式を用いた配信システムにおいて、鍵ペアの更新は個々の受信側が個別に行うよりも、配信側や鍵管理センタ等が総合的な見地から必要と判断した時に行うことが望ましく、また、配信側や鍵管理センタ等において公開鍵を効率よく管理するために所定の時期に全ての鍵ペアの更新を一斉に行うことも望まれるが、従来の公開鍵

暗号方式を用いた配信システムでは、鍵ペアの更新の主導権を各受信側が持っているので、現状ではいずれの実現も難しい。

【0009】本発明は、公開鍵暗号方式を用いた配信システムにおいて、配信側や鍵管理センタが鍵ペアの更新の主導権を持ち、また鍵ペアの更新を一斉に行うことができる更新方法、受信端末及び鍵管理装置を提供することを目的とする。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明に係る更新方法は、鍵管理センタと配信局と1つ以上の受信端末とを含むデータ配信システムにおいて公開鍵暗号方式の鍵ペアをなす配信用公開鍵及び配信用秘密鍵を更新する更新方法であって、配信用公開鍵は配信すべきデータを暗号化して暗号化データを生成する際に用いられ、配信用秘密鍵は配信された暗号化データを復号する際に用いられ、当該更新方法は、所定の受信端末においてデータ配信を始める前に更新用秘密鍵を入手する秘密鍵入手ステップと、前記鍵管理センタにおいてデータ配信を始める前に前記更新用秘密鍵と鍵ペアをなす更新用公開鍵を入手する公開鍵入手ステップと、前記鍵管理センタにおいて前記受信端末用に配信用公開鍵及び配信用秘密鍵を生成する生成ステップと、前記鍵管理センタにおいて前記生成ステップにより生成された配信用秘密鍵を前記公開鍵入手ステップにより入手された更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成する暗号化ステップと、前記鍵管理センタにおいて任意のタイミングで前記暗号化ステップにより生成された暗号化秘密鍵を前記受信端末へ向けて送出する送出ステップと、前記鍵管理センタにおいて前記送出ステップにより暗号化秘密鍵が前記受信端末へ向けて送出された後はデータ配信の際に配信局により使用される当該受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成手段により当該受信端末用に生成された配信用公開鍵に更新する公開鍵更新ステップと、前記受信端末において前記送出ステップにより送出された暗号化秘密鍵を受付ける受け付けステップと、前記受信端末において前記受け付けステップにより暗号化秘密鍵が受け付けられた後は当該受信端末用の配信用秘密鍵をそれまで使用していた配信用秘密鍵から前記秘密鍵入手ステップにより入手された更新用秘密鍵を用いて当該暗号化秘密鍵を必要に応じて復号することにより復元される配信用秘密鍵に更新する秘密鍵更新ステップとを含むことを特徴とする。

【0011】これによって、鍵管理センタが配信用公開鍵、及び、配信用秘密鍵を生成し、配信用秘密鍵を更新用公開鍵を用いて暗号化して送出することができる。従って、鍵配送時の安全性を損なわずに、鍵管理センタが配信用鍵ペアの更新の主導権を持つことができる。上記目的を達成するために、本発明に係る受信端末は、所定

データが当該受信端末用の配信用公開鍵を用いて暗号化されることにより生成された配信局から配信される暗号化データを受信して当該暗号化データを当該受信端末用の配信用秘密鍵を用いて復号して前記所定データを得る受信端末であって、データ配信を始める前に更新用秘密鍵を入手する秘密鍵入手手段と、当該受信端末用の配信用秘密鍵が前記更新用秘密鍵と鍵ペアをなす更新用公開鍵を用いて暗号化されることにより生成された暗号化秘密鍵を保持する保持手段と、前記配信局より配信される前記暗号化データを受信する受信手段と、前記保持手段に保持されている暗号化秘密鍵を前記秘密鍵入手手段により入手された更新用秘密鍵を用いて復号して当該受信端末用の配信用秘密鍵を復元する秘密鍵復号手段と、前記受信手段により受信された暗号化データを前記秘密鍵復号手段により復元された配信用秘密鍵を用いて復号して前記所定データを得るデータ復号手段とを備えることを特徴とする。

【0012】これによって、保持している暗号化秘密鍵を、入手された源秘密鍵を用いて復号して配信用秘密鍵を生成し、受信した暗号化データを、生成した配信用秘密鍵を用いて復号して、前記所定データを得ることができる。従って、源秘密鍵を各受信端末において秘密に入手することができさえすれば、配信用秘密鍵を受信端末以外が容易に更新することができるので、鍵配送時の安全性を損なわずに、受信端末以外に配信用鍵ペアの更新の主導権を持たせることができる。

【0013】上記目的を達成するために、本発明に係る鍵管理装置は、データ配信を始める前に更新用秘密鍵を保持している所定の受信端末用に当該更新用秘密鍵と鍵ペアをなす更新用公開鍵を入手する公開鍵入手手段と、前記受信端末用に公開鍵暗号方式の鍵ペアをなす配信用公開鍵及び配信用秘密鍵を生成する生成手段と、前記生成手段により生成された配信用秘密鍵を前記公開鍵入手手段により入手された更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成する暗号化手段と、任意のタイミングで前記暗号化手段により生成された暗号化秘密鍵を前記受信端末へ向けて送出する送出手段と、前記送出手段により暗号化秘密鍵が前記受信端末へ向けて送出された後はデータ配信の際に使用される当該受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成手段により当該受信端末用に生成された配信用公開鍵に更新する公開鍵更新手段とを備えることを特徴とする。

【0014】これによって、鍵管理装置が配信用公開鍵、及び、配信用秘密鍵を生成し、配信用秘密鍵を更新用公開鍵を用いて暗号化して送出することができる。従って、鍵配送時の安全性を損なわずに、鍵管理装置が配信用鍵ペアの更新の主導権を持つことができる。

【0015】

【発明の実施の形態】（実施の形態1）

＜概要＞本発明の実施の形態１は、１つの鍵管理センタ、１つの配信局、及び、複数の受信端末を含むコンテンツの配信システムにおいて、鍵管理センタが主導的に、配信用の鍵ペアを安全に更新する技術を説明する。

【００１６】配信を始める前に予め各受信端末が更新用秘密鍵と更新用公開鍵との鍵ペアを生成して、更新用秘密鍵を秘密に保持し、更新用公開鍵を鍵管理センタに渡しておく。鍵管理センタは、予め各受信端末から渡された更新用公開鍵を保持しておき、最初及び鍵更新時に、受信端末毎に配信用秘密鍵と配信用公開鍵との鍵ペアを生成して、生成した配信用公開鍵を配信局によるコンテンツの配信に用いさせることにし、生成した配信用秘密鍵を保持しておいた更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成して各受信端末に送る。

【００１７】各受信端末は、暗号化秘密鍵を受け取って、この暗号化秘密鍵を予め保持しておいた更新用秘密鍵を用いて復号して配信用秘密鍵を生成し、コンテンツの配信時に用いる。このように、配信用秘密鍵を更新用公開鍵を用いて暗号化した状態で送るので、配信用秘密鍵を安全に送ることができ、且つ、鍵管理センタが主導的に、配信用の鍵ペアを更新することができる。

【００１８】＜構成＞図１は、本発明の実施の形態１の配信システムを示す図である。図１に示す配信システム１００は、鍵管理センタ装置１１０、配信局装置１２０、受信端末１３０、受信端末１４０、及び、受信端末１５０から構成される。鍵管理センタ装置１１０は、鍵管理センタにおいて配信システム１００を構成する全ての受信端末用の鍵を管理する装置であり、公開鍵管理部１１１、配信用鍵生成部１１２、暗号化部１１３、送出部１１４、公開鍵更新部１１５、認知部１１６、配信禁止部１１７を備える。

【００１９】配信局装置１２０は、配信局において配信データを生成して各受信端末へ配信する装置であり、配信データ生成部１２１、配信部１２２を備える。受信端末１３０は、コンテンツ利用者の元において、配信局より配信された配信データを受信し再生する端末であり、更新用鍵生成部１３１、秘密鍵管理部１３２、保持部１３３、受信部１３４、秘密鍵復号部１３５、コンテンツ復号部１３６、受け付け部１３７、秘密鍵更新部１３８を備える。

【００２０】ここで、受信端末１４０、及び、受信端末１５０は、受信端末１３０と同様なので、その説明を省略する。公開鍵管理部１１１は、配信を始める前に、それぞれの受信端末用のそれぞれユニークな更新用公開鍵を、各受信端末から入手して管理する。配信用鍵生成部１１２は、配信を始める前及び鍵更新時に、それぞれの受信端末用に、それぞれユニークな、公開鍵暗号方式の鍵ペアである配信用公開鍵、及び、配信用秘密鍵を生成する。

【００２１】本明細書では公開鍵暗号方式として、Ｅ１

Ｇａｍａ１暗号方式を用いるものとする。Ｅ１Ｇａｍａ１暗号方式については、池野信一、小山謙二著「現代暗号理論」（電子情報通信学会）に詳しく記載されている。暗号化部１１３は、配信用鍵生成部１１２により、それぞれの受信端末用に生成された配信用秘密鍵を、公開鍵管理部１１１により管理されているそれぞれの受信端末用の更新用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化秘密鍵を生成し、さらに、鍵管理センタ装置１１０を示し当該暗号化秘密鍵の正当性を示すデジタル署名を施す。

【００２２】本明細書ではデジタル署名の方式として、Ｅ１Ｇａｍａ１暗号方式を用いた署名方式を用いるものとする。Ｅ１Ｇａｍａ１暗号方式を用いた署名方式については、池野信一、小山謙二著「現代暗号理論」（電子情報通信学会）に詳しく記載されている。送出部１１４は、配信を始める前及び鍵更新時に、暗号化部１１３により生成されたそれぞれの受信端末用の暗号化秘密鍵を、それぞれ対応する受信端末へ向けて送出する。

【００２３】公開鍵更新部１１５は、送出部１１４によりそれぞれの受信端末用の暗号化秘密鍵がそれぞれ対応する受信端末へ向けて送出された後は、配信用鍵生成部１１２によりそれぞれの受信端末用に生成された配信用公開鍵を、それぞれの受信端末用の配信用公開鍵として、データ配信の際に用いるように、配信局装置１２０に指示する。

【００２４】認知部１１６は、受信端末毎に不正なく正常に稼動しているかを監視し、データ配信を中止すべき受信端末や、配信用秘密鍵を更新すべき受信端末を認知する。例えば、認知部１１６は、一部の受信端末が正常に稼動していない場合や、定期的に、全ての配信用秘密鍵を更新すべきであると認知してもよい。ここで認知部１１６により更新すべきであると認知された配信用秘密鍵は、配信用鍵生成部１１２、暗号化部１１３、送出部１１４、及び、公開鍵更新部１１５により遅滞なく更新される。

【００２５】配信禁止部１１７は、認知部１１６によりデータ配信を中止すべき受信端末が認知された以後は、当該受信端末用の配信用公開鍵を用いたデータ配信を禁止する。配信データ生成部１２１は、秘密鍵暗号方式の鍵であるコンテンツ鍵を、それぞれの受信端末用の配信用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化コンテンツ鍵を生成し、配信すべきコンテンツを、コンテンツ鍵を用いて暗号化して暗号化コンテンツを生成する。

【００２６】ここで、配信禁止部１１７により、特定の受信端末に対してデータ配信が禁止されている場合には、配信データ生成部１２１は、コンテンツ鍵を当該特定の受信端末用の配信用公開鍵を用いて暗号化した当該特定の受信端末用の暗号化コンテンツ鍵を生成しない。配信部１２２は、配信データ生成部１２１により生成さ

れたそれぞれの受信端末用の暗号化コンテンツ鍵の全てと暗号化コンテンツとを、全ての受信端末へ配信する。

【0027】更新用鍵生成部131は、配信を始める前に、当該受信端末用に、公開鍵暗号方式の鍵ペアである更新用秘密鍵と更新用公開鍵とを生成して、更新用秘密鍵は秘密に秘密鍵管理部132に渡し、更新用公開鍵は特に秘密にすることなく公開鍵管理部111へ渡す。秘密鍵管理部132は、更新用鍵生成部131により生成された更新用秘密鍵を秘密に入手して管理する。

【0028】保持部133は、当該受信端末用の配信用秘密鍵が、当該受信端末用の更新用公開鍵を用いて暗号化されることにより生成された暗号化秘密鍵を保持する。ここで、保持部133に保持されている暗号化秘密鍵には、鍵管理センタ装置110を示し当該暗号化秘密鍵の正当性を示すデジタル署名が施されている。受信部134は、配信局より配信されるそれぞれの受信端末用の暗号化コンテンツ鍵の全てと暗号化コンテンツとを受信する。

【0029】秘密鍵復号部135は、保持部133に保持されている暗号化秘密鍵を、秘密鍵管理部132により管理されている更新用秘密鍵を用いて復号して、当該受信端末用の配信用秘密鍵を生成する。ここで、秘密鍵復号部135は、保持部133に保持されている暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が鍵管理センタ装置110に対応する正当なものであるか否かを判断し、正当なものであると判断した場合に当該受信端末用の配信用秘密鍵を生成し、正当なものではないと判断した場合に当該受信端末用の配信用秘密鍵を生成しない。

【0030】コンテンツ復号部136は、受信部134により受信された暗号化コンテンツ鍵を、秘密鍵復号部135により生成された配信用秘密鍵を用いて復号してコンテンツ鍵を生成し、受信部134により受信された暗号化コンテンツを、生成したコンテンツ鍵を用いて復号してコンテンツを得る。受け部137は、送出处114から送出される暗号化秘密鍵を受付ける。

【0031】秘密鍵更新部138は、受け部137により暗号化秘密鍵が受けられた後は、受けられた暗号化秘密鍵を保持部133に保持させる。ここで秘密鍵更新部138は、既に保持部133に暗号化秘密鍵が保持されている場合には、保持された暗号化秘密鍵を、受けられた暗号化秘密鍵で更新する。

【0032】また秘密鍵更新部138は、受け部137により受けられた暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が鍵管理センタ装置110に対応する正当なものであるか否かを判断し、正当なものであると判断した場合に配信用秘密鍵を更新し、正当なものではないと判断した場合に配信用秘密鍵を更新しない。

【0033】<動作>図2は、コンテンツの配信を始め

る前に予め行う準備の手順を示す図である。以下に、図2を用いて予め行う準備の手順を説明する。

(1) 各受信端末において、更新用秘密鍵と更新用公開鍵との鍵ペアを生成して、更新用秘密鍵を秘密に保持し、更新用公開鍵を鍵管理センタ装置に渡す(ステップS1)。例えば受信端末130において、更新用鍵生成部131が、更新用秘密鍵IKs1と更新用公開鍵IKp1との鍵ペアを生成して、更新用秘密鍵IKs1は秘密に秘密鍵管理部132に渡し、更新用公開鍵IKp1は特に秘密にすることなく一般通信回線等を介して公開鍵管理部111へ渡す。秘密鍵管理部132は更新用秘密鍵IKs1を入手して秘密に管理する。

【0034】同様に受信端末140において、更新用秘密鍵IKs2と更新用公開鍵IKp2との鍵ペアを生成して、更新用秘密鍵IKs2を秘密に管理し、更新用公開鍵IKp2を公開鍵管理部111へ渡す。同様に受信端末150において、更新用秘密鍵IKs3と更新用公開鍵IKp3との鍵ペアを生成して、更新用秘密鍵IKs3を秘密に管理し、更新用公開鍵IKp3は公開鍵管理部111へ渡す。

【0035】(2) 鍵管理センタにおいて、それぞれの受信端末から入手した各更新用公開鍵を管理する(ステップS2)。例えば公開鍵管理部111が、受信端末130用の更新用秘密鍵IKs1と、受信端末140用の更新用秘密鍵IKs2と、受信端末150用の更新用秘密鍵IKs3とを入手して管理する。

(3) 鍵管理センタにおいて、各受信端末毎に、配信用秘密鍵と配信用公開鍵との鍵ペアを生成する(ステップS3)。例えば配信用鍵生成部112が、受信端末130用の配信用公開鍵Kp1と配信用秘密鍵Ks1との鍵ペア、受信端末140用の配信用公開鍵Kp2と配信用秘密鍵Ks2との鍵ペア、受信端末150用の配信用公開鍵Kp3と配信用秘密鍵Ks3との鍵ペアを生成する。

【0036】(4) 鍵管理センタにおいて、各受信端末毎に生成された配信用秘密鍵を、それぞれの受信端末用の更新用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化秘密鍵を生成し、さらに、デジタル署名を施す(ステップS4)。例えば暗号化部113が、受信端末130用に配信用秘密鍵Ks1を更新用公開鍵IKp1を用いて暗号化して暗号化秘密鍵E(IKp1、Ks1)を生成し、受信端末140用に配信用秘密鍵Ks2を更新用公開鍵IKp2を用いて暗号化して暗号化秘密鍵E(IKp2、Ks2)を生成し、受信端末150用に配信用秘密鍵Ks3を更新用公開鍵IKp3を用いて暗号化して暗号化秘密鍵E(IKp3、Ks3)を生成する。

【0037】(5) 鍵管理センタにおいて、それぞれの受信端末用の暗号化秘密鍵を、それぞれ対応する受信端末へ向けて送出する(ステップS5)。例えば送出处1

14が、暗号化秘密鍵E（IKp1、Ks1）を受信端末130へ向けて送出し、暗号化秘密鍵E（IKp2、Ks2）を受信端末140へ向けて送出し、暗号化秘密鍵E（IKp3、Ks3）を受信端末150へ向けて送出する。

【0038】（6）鍵管理センタにおいて、各受信端末毎の配信用公開鍵の全てをコンテンツの配信時に用いるよう配信局に指示する（ステップS6）。例えば配信用公開鍵Kp1、配信用公開鍵Kp2、配信用公開鍵Kp3をコンテンツの配信時に用いるよう配信局装置120中の配信データ生成部121に指示する。

（7）各受信端末において、暗号化秘密鍵を受付ける（ステップS7）。例えば受信端末130において、受付け部137が暗号化秘密鍵E（IKp1、Ks1）を受付ける。

【0039】同様に受信端末140において、暗号化秘密鍵E（IKp2、Ks2）を受付ける。同様に受信端末150において、暗号化秘密鍵E（IKp3、Ks3）を受付ける。

（8）各受信端末において、受付けられた暗号化秘密鍵を保持する（ステップS8）。例えば受信端末130において、秘密鍵更新部138が、受付け部137により受付けられた暗号化秘密鍵E（IKp1、Ks1）を保持部133に保持させる。

【0040】同様に受信端末140において、暗号化秘密鍵E（IKp2、Ks2）を保持する。同様に受信端末150において、暗号化秘密鍵E（IKp3、Ks3）を保持する。図3は、コンテンツの配信時の手順を示す図である。

【0041】以下に、図3を用いてコンテンツの配信時の手順を説明する。

（1）配信局において、コンテンツをコンテンツ鍵を用いて暗号化して暗号化コンテンツを生成し、コンテンツ鍵を鍵管理センタ装置が管理する各受信端末用の配信用公開鍵を用いて暗号化して各受信端末用の暗号化コンテンツ鍵を生成する（ステップS21）。例えば配信データ生成部121が、配信すべきコンテンツMをコンテンツ鍵Kを用いて暗号化して暗号化コンテンツCを生成し、コンテンツ鍵Kを受信端末130用の配信用公開鍵Kp1を用いて暗号化して暗号化コンテンツ鍵E（Kp1、K）を生成し、コンテンツ鍵Kを受信端末140用の配信用公開鍵Kp2を用いて暗号化して暗号化コンテンツ鍵E（Kp2、K）を生成し、コンテンツ鍵Kを受信端末150用の配信用公開鍵Kp3を用いて暗号化して暗号化コンテンツ鍵E（Kp3、K）を生成する。

【0042】（2）配信局において、暗号化コンテンツと全ての暗号化コンテンツ鍵とを各受信端末に配信する（ステップS22）。例えば配信部122が、暗号化コンテンツCと暗号化コンテンツ鍵E（Kp1、K）と暗号化コンテンツ鍵E（Kp2、K）と暗号化コンテンツ

鍵E（Kp3、K）とを、受信端末130と受信端末140と受信端末150とへ配信する。

【0043】（3）各受信端末において、配信局より配信される暗号化コンテンツ鍵とそれぞれの受信端末用の暗号化コンテンツ鍵の全てを受信する（ステップS23）。例えば受信端末130において、受信部134が暗号化コンテンツCと暗号化コンテンツ鍵E（Kp1、K）と暗号化コンテンツ鍵E（Kp2、K）と暗号化コンテンツ鍵E（Kp3、K）とを受信する。

【0044】（4）各受信端末において、保持されている暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が正当なものであるか否かを判断する（ステップS24）。例えば受信端末130において、秘密鍵復号部135が保持部133に保持されている暗号化秘密鍵E（IKp1、Ks1）に施されたデジタル署名に基づいて、当該暗号化秘密鍵が正当なものであるか否かを判断し、正当なものであると判断されなかった場合にはコンテンツの再生をせずに処理を終了する。

【0045】（5）各受信端末において、保持されている暗号化秘密鍵が正当なものであると判断された場合には、当該暗号化秘密鍵を更新用秘密鍵を用いて復号して配信用秘密鍵を生成する（ステップS25）。例えば受信端末130において、秘密鍵復号部135が保持部133に保持されている暗号化秘密鍵E（IKp1、Ks1）を、秘密鍵管理部132により管理されている更新用秘密鍵IKs1を用いて復号して配信用秘密鍵Ks1を生成する。

【0046】（6）各受信端末において、受信された暗号化コンテンツ鍵を、生成された配信用秘密鍵を用いて復号してコンテンツ鍵を生成し、受信された暗号化コンテンツを、生成したコンテンツ鍵を用いて復号してコンテンツを得る（ステップS26）。例えば受信端末130において、コンテンツ復号部136が受信部134により受信された暗号化コンテンツ鍵E（Kp1、K）を、秘密鍵復号部135により生成された配信用秘密鍵Ks1を用いて復号してコンテンツ鍵Kを生成し、受信部134により受信された暗号化コンテンツCを、生成したコンテンツ鍵Kを用いて復号してコンテンツMを得る。

【0047】図4は、鍵更新時の手順を示す図である。以下に、図4を用いて鍵更新時の手順を説明する。

（1）鍵管理センタにおいて、受信端末毎に不正なく正常に稼動しているかを監視し、配信用秘密鍵を更新すべき受信端末を認知する（ステップS31）。例えば、認知部116が、受信端末130、受信端末140、受信端末150用の配信用秘密鍵を更新すべきであると認知する。

【0048】（2）鍵管理センタにおいて、各受信端末毎に、配信用秘密鍵と配信用公開鍵との鍵ペアを生成する（ステップS32）。例えば配信用鍵生成部112

が、受信端末130用の配信用公開鍵 $K_{p11}$ と配信用秘密鍵 $K_{s11}$ との鍵ペア、受信端末140用の配信用公開鍵 $K_{p12}$ と配信用秘密鍵 $K_{s12}$ との鍵ペア、受信端末150用の配信用公開鍵 $K_{p13}$ と配信用秘密鍵 $K_{s13}$ との鍵ペアを生成する。

【0049】(3) 鍵管理センタにおいて、各受信端末毎に生成された配信用秘密鍵を、それぞれの受信端末用の更新用公開鍵を用いて暗号化して、それぞれの受信端末用の暗号化秘密鍵を生成し、さらに、デジタル署名を施す(ステップS33)。例えば暗号化部113が、受信端末130用に配信用秘密鍵 $K_{s11}$ を更新用公開鍵 $I_{Kp1}$ を用いて暗号化して暗号化秘密鍵 $E(I_{Kp1}, K_{s11})$ を生成し、受信端末140用に配信用秘密鍵 $K_{s12}$ を更新用公開鍵 $I_{Kp2}$ を用いて暗号化して暗号化秘密鍵 $E(I_{Kp2}, K_{s12})$ を生成し、受信端末150用に配信用秘密鍵 $K_{s13}$ を更新用公開鍵 $I_{Kp3}$ を用いて暗号化して暗号化秘密鍵 $E(I_{Kp3}, K_{s13})$ を生成する。

【0050】(4) 鍵管理センタにおいて、それぞれの受信端末用の暗号化秘密鍵を、それぞれ対応する受信端末へ向けて送出する(ステップS34)。例えば送出部114が、暗号化秘密鍵 $E(I_{Kp1}, K_{s11})$ を受信端末130へ向けて送出し、暗号化秘密鍵 $E(I_{Kp2}, K_{s12})$ を受信端末140へ向けて送出し、暗号化秘密鍵 $E(I_{Kp3}, K_{s13})$ を受信端末150へ向けて送出する。

【0051】(5) 鍵管理センタにおいて、各受信端末毎の配信用公開鍵の全てをコンテンツの配信時に用いるよう配信局に指示する(ステップS35)。例えば配信用公開鍵 $K_{p11}$ 、配信用公開鍵 $K_{p12}$ 、配信用公開鍵 $K_{p13}$ をコンテンツの配信時に用いるよう配信局装置120中の配信データ生成部121に指示する。

(6) 各受信端末において、暗号化秘密鍵を受付ける(ステップS36)。例えば受信端末130において、受け付け部137が暗号化秘密鍵 $E(I_{Kp1}, K_{s11})$ を受付ける。

【0052】同様に受信端末140において、暗号化秘密鍵 $E(I_{Kp2}, K_{s12})$ を受付ける。同様に受信端末150において、暗号化秘密鍵 $E(I_{Kp3}, K_{s13})$ を受付ける。

(7) 各受信端末において、暗号化秘密鍵が受け付けられた後は、保持された暗号化秘密鍵を、受け付けられた暗号化秘密鍵で更新する(ステップS37)。例えば受信端末130において、秘密鍵更新部138が、保持部133に保持された暗号化秘密鍵 $E(I_{Kp1}, K_{s11})$ を、受け付け部137により受け付けられた暗号化秘密鍵 $E(I_{Kp1}, K_{s11})$ に更新する。

【0053】同様に受信端末140において、暗号化秘密鍵 $E(I_{Kp2}, K_{s12})$ を、暗号化秘密鍵 $E(I_{Kp2}, K_{s12})$ に更新する。同様に受信端末150に

おいて、暗号化秘密鍵 $E(I_{Kp3}, K_{s13})$ を、暗号化秘密鍵 $E(I_{Kp3}, K_{s13})$ に更新する。なお、鍵管理センタ装置と配信局装置とは同一の装置であってもよい。

【0054】以上のように、本発明の実施の形態1によれば、配信局や鍵管理センタが主導的に、配信用の鍵ペアを更新することができる。

(実施の形態2)

<概要>本発明の実施の形態2は、機器メーカー、DVD再生機器、鍵管理センタ、ICカード、コンテンツメーカー、ディスク制作者、及び、DVDディスクからなるDVDディスクの配信システムにおいて、鍵管理センタが主導的に、配信用の鍵ペアを安全に更新する技術を説明する。

【0055】機器メーカーがDVD再生機器の製造時に、DVD再生機器毎にユニークな初期秘密鍵と初期公開鍵との鍵ペアを生成して、この初期秘密鍵をDVD再生機器に秘密に保持させ、この初期公開鍵を鍵管理センタに渡す。鍵管理センタは、機器メーカーから渡された初期公開鍵を対応するDVD再生機器用としてデータベースに登録し、このDVD再生機器用に配信用秘密鍵と配信用公開鍵との鍵ペアを生成して、生成した配信用公開鍵をデータベースに登録してディスク制作者によるDVDディスクの製造に用いさせることにし、生成した配信用秘密鍵を登録しておいたこのDVD再生機器用の初期公開鍵を用いて暗号化して暗号化秘密鍵を生成して機器メーカーに送り返す。

【0056】機器メーカーは、暗号化秘密鍵を受け取ってICカードに記録し、このICカードをこのDVD再生機器とセットで販売する。鍵管理センタは、DVDディスクの配信を開始した後に鍵更新が必要だと判断すると、所定のDVD再生機器用に配信用秘密鍵と配信用公開鍵との鍵ペアを新たに生成して、予めデータベースに登録してある当該DVD再生機器用の配信用公開鍵を、生成した配信用公開鍵で更新し、生成した配信用秘密鍵を登録しておいた当該DVD再生機器用の初期公開鍵を用いて暗号化して暗号化秘密鍵を生成して新しいICカードに記録し、このICカードをこのDVD再生機器の元へ届ける。

【0057】所定のDVD再生機器の元へ、新しいICカードが届くと、元のICカードを新しいICカードと差し換え、以後のDVDディスクの再生に用いる。このように、配信用秘密鍵を初期公開鍵を用いて暗号化した状態でICカードに記録して送るので、配信用秘密鍵を安全に送ることができ、且つ、鍵管理センタが主導的に、配信用の鍵ペアを更新することができる。

【0058】<構成>図5は、本発明の実施の形態2のDVD再生機器の製造システムを示す図である。図5に示す製造システム200は、機器メーカー装置210、DVD再生機器220、ICカード230、鍵管理センタ

装置240から構成される。

【0059】機器メーカ装置210は、機器メーカにおいてDVD再生機器220を製造する装置であり、初期鍵生成部211、鍵書込み部212、公開鍵伝送部213、ICカード記録部214を備える。DVD再生機器220は、コンテンツ利用者の元においてDVDディスクを再生する装置であり、秘密鍵記録部221を備える。

【0060】ICカード230は、DVD再生機器の製造時に機器メーカ装置210のICカードスロットに挿入されて必要なデータが書き込まれ、DVD再生機器220と共にセットで販売され、DVDディスクの再生時にDVD再生機器220のICカードスロットに挿入されて使用される半導体記録媒体である。鍵管理センタ装置240は、鍵管理センタにおいて配信システムを構成する全てのDVD再生機器用の鍵を管理する装置であり、初期公開鍵登録部241、配信用鍵生成部242、秘密鍵暗号化部243、送出部244、配信用公開鍵登録部245、初期公開鍵データベース246、配信用公開鍵データベース247を備える。

【0061】初期鍵生成部211は、DVD再生機器220用に、公開鍵暗号方式の鍵ペアである初期秘密鍵と初期公開鍵とを生成する。鍵書込み部212は、初期鍵生成部211により生成された初期秘密鍵を秘密鍵記録部221に書込む。公開鍵伝送部213は、初期鍵生成部211により生成された初期公開鍵をオフラインで初期公開鍵登録部241へ伝送する。

【0062】ICカード記録部214は、DVD再生機器220用の配信用秘密鍵が、秘密鍵暗号化部243によりDVD再生機器220用の初期公開鍵を用いて暗号化されることにより生成された暗号化秘密鍵を送出部244より入手してICカード230に記録して、DVD再生機器220と共に出荷する。秘密鍵記録部221は、鍵書込み部212により初期秘密鍵を書き込まれ、当該初期秘密鍵を秘密に記録する。

【0063】初期公開鍵登録部241は、公開鍵伝送部213より伝送された初期公開鍵を入手して初期公開鍵データベース246に登録する。配信用鍵生成部242は、所定のDVD再生機器の製造時及び鍵更新時に、当該DVD再生機器用にユニークな、公開鍵暗号方式の鍵ペアである配信用公開鍵、及び、配信用秘密鍵を生成する。

【0064】秘密鍵暗号化部243は、配信用鍵生成部242により所定のDVD再生機器用に生成された配信用秘密鍵を、初期公開鍵データベース246に登録されている当該DVD再生機器用の初期公開鍵を用いて暗号化して、当該DVD再生機器用の暗号化秘密鍵を生成し、さらに、鍵管理センタ装置240を示し当該暗号化秘密鍵の正当性を示すデジタル署名を施す。

【0065】送出部244は、所定のDVD再生機器の

製造時に、秘密鍵暗号化部243により生成された当該DVD再生機器用の暗号化秘密鍵を、当該DVD再生機器へ向けて送出する。配信用公開鍵登録部245は、送出部244により所定のDVD再生機器用の暗号化秘密鍵が送出された後、及び、新しいICカード作成部344により新しいICカードが当該DVD再生機器へ向けて送出された後に、配信用鍵生成部242により生成された配信用公開鍵を配信用公開鍵データベース247に登録する。

【0066】初期公開鍵データベース246は、初期公開鍵登録部241により登録された初期公開鍵をDVD再生機器別に記録する。配信用公開鍵データベース247は、配信用公開鍵登録部245により登録された配信用公開鍵をDVD再生機器別に記録する。図6は、本発明の実施の形態2の配信システムを示す図である。

【0067】図6に示す配信システム300は、DVD再生機器220、ICカード330、鍵管理センタ装置240、コンテンツメーカ装置350、ディスク制作装置360、及び、DVDディスク370から構成される。DVD再生機器220は、上記に示した秘密鍵記録部221に、さらに、秘密鍵復号部321、コンテンツ鍵復号部322、コンテンツ復号部323、ICカード更新部324を備える。

【0068】ICカード330は、鍵更新時に鍵管理センタ装置240のICカードスロットに挿入されて必要なデータが書き込まれ、後のDVDディスクの再生時にDVD再生機器220のICカードスロットに挿入されて使用される半導体記録媒体である。鍵管理センタ装置240は、上記に示した初期公開鍵登録部241、配信用鍵生成部242、秘密鍵暗号化部243、送出部244、配信用公開鍵登録部245、初期公開鍵データベース246、配信用公開鍵データベース247に、さらに、コンテンツ鍵暗号化部341、認知部342、登録抹消部343、新しいICカード作成部344を備える。

【0069】コンテンツメーカ装置350は、コンテンツメーカにおいてコンテンツとコンテンツ鍵とを提供する装置であり、コンテンツ鍵管理部351、コンテンツ管理部352を備える。ディスク制作装置360は、ディスク制作者においてDVDディスク370を制作する装置であり、コンテンツ鍵受渡し部361、コンテンツ暗号化部362、暗号化コンテンツ鍵受渡し部363、制作部364を備える。

【0070】DVDディスク370は、ディスク制作者においてディスク制作装置360により制作され、コンテンツ利用者の元においてDVD再生機器220により再生される光記録媒体である。秘密鍵復号部321は、DVDディスクの再生時に、DVD再生機器220のICカードスロットに挿入されたICカード230又はICカード330から暗号化秘密鍵を読み出し、当該暗号化秘密鍵を、秘密鍵記録部221に記録されている初

期秘密鍵を用いて復号して配信用秘密鍵を生成する。

【0071】ここで、秘密鍵復号部321は、暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が鍵管理センタ装置240に対応する正当なものであるか否かを判断し、正当なものであると判断した場合にDVD再生機器220用の配信用秘密鍵を生成し、正当なものではないと判断した場合にDVD再生機器220用の配信用秘密鍵を生成しない。

【0072】コンテンツ鍵復号部322は、DVDディスクの再生時に、DVDディスク370に記録されたDVD再生機器220用の暗号化コンテンツ鍵を、秘密鍵復号部321により生成された配信用秘密鍵を用いて復号してコンテンツ鍵を生成する。コンテンツ復号部323は、DVDディスク370に記録された暗号化コンテンツを、コンテンツ鍵復号部322により生成されたコンテンツ鍵を用いて復号してコンテンツを得る。

【0073】ICカード更新部324は、新ICカード作成部344からICカード330を受付けた後は、DVD再生機器220のICカードスロットにICカード330を挿入して、以後のDVDディスクの再生に備える。コンテンツ鍵暗号化部341は、DVDディスクの製造時に、コンテンツ鍵受渡し部361から、当該DVDディスクの製造時に用いるコンテンツ鍵を受け取り、当該コンテンツ鍵を、配信用公開鍵データベース247に記録された現時点において有効な全てのDVD再生機器用の配信用公開鍵をそれぞれ用いて暗号化して、それぞれのDVD再生機器用の暗号化コンテンツ鍵を生成して、暗号化コンテンツ鍵受渡し部363に渡す。

【0074】認知部342は、DVD再生機器毎に正しく正常に稼動しているかを監視し、DVDディスクの再生を禁止すべきDVD再生機器や、配信用秘密鍵を更新すべきDVD再生機器を認知する。例えば、認知部342は、一部のDVD再生機器が正常に稼動していない場合や、定期的に、全ての配信用秘密鍵を更新すべきであると認知してもよい。

【0075】ここで認知部342により更新すべきであると認知された配信用秘密鍵は、新ICカード作成部344により新しいICカードが対応するDVD再生機器へ向けて送出された後に遅滞なく、配信用鍵生成部242、秘密鍵暗号化部243、及び、配信用公開鍵登録部245により更新される。登録抹消部343は、認知部342によりDVDディスクの再生を禁止すべきDVD再生機器が認知された以後は、当該DVD再生機器用の配信用公開鍵を、配信用公開鍵データベース247から抹消する。

【0076】新ICカード作成部344は、所定のDVD再生機器の鍵更新時に、秘密鍵暗号化部243により生成された当該DVD再生機器用の暗号化秘密鍵を、新しいICカードに記録してICカード330を作成し、当該DVD再生機器へ向けて送出する。コンテンツ鍵管

理部351は、コンテンツ鍵を管理し、現時点において有効なコンテンツ鍵をディスク制作装置360へ供給する。

【0077】コンテンツ管理部352は、コンテンツを管理し、供給すべきコンテンツをディスク制作装置360へ供給する。コンテンツ鍵受渡し部361は、コンテンツ鍵管理部351よりコンテンツ鍵の供給を受け、コンテンツ鍵暗号化部341に渡す。コンテンツ暗号化部362は、コンテンツ管理部352よりコンテンツの供給を受け、コンテンツ鍵受渡し部361からコンテンツ鍵の供給を受け、当該コンテンツを当該コンテンツ鍵を用いて暗号化して暗号化コンテンツを生成して制作部364へ渡す。

【0078】暗号化コンテンツ鍵受渡し部363は、コンテンツ鍵暗号化部341から、それぞれのDVD再生機器用の暗号化コンテンツ鍵の供給を受け、制作部364へ渡す。制作部364は、コンテンツ暗号化部362から渡された暗号化コンテンツと、暗号化コンテンツ鍵受渡し部363から渡されたそれぞれのDVD再生機器用の暗号化コンテンツ鍵とを記録したDVDディスク370を制作する。

【0079】＜動作＞図7は、DVD再生機器の製造時の手順を示す図である。以下に、図7を用いてDVD再生機器の製造時の手順を説明する。

(1) 機器メーカーにおいて、DVD再生機器220の製造時に、初期鍵生成部211がDVD再生機器220用に初期秘密鍵と初期公開鍵とを生成する(ステップS41)。

【0080】(2) 機器メーカーにおいて、鍵書込み部212がDVD再生機器220用の初期秘密鍵を秘密鍵記録部221に書込む(ステップS42)。

(3) 機器メーカーにおいて、公開鍵伝送部213がDVD再生機器220用の初期公開鍵を初期公開鍵登録部241へ伝送する(ステップS43)。

(4) 鍵管理センタにおいて、初期公開鍵登録部241がDVD再生機器220用の初期公開鍵を入手して初期公開鍵データベース246に登録する(ステップS44)。

【0081】(5) 鍵管理センタにおいて、配信用鍵生成部242がDVD再生機器220用の配信用秘密鍵及び配信用公開鍵を生成する(ステップS45)。

(6) 鍵管理センタにおいて、秘密鍵暗号化部243が生成されたDVD再生機器220用の配信用秘密鍵を、初期公開鍵データベース246に登録されているDVD再生機器220用の初期公開鍵を用いて暗号化して、暗号化秘密鍵を生成し、さらにデジタル署名を施す(ステップS46)。

【0082】(7) 鍵管理センタにおいて、送出部244がDVD再生機器220用に生成されたデジタル署名付き暗号化秘密鍵をDVD再生機器220へ向けて送出

する（ステップS 4 7）。

（8）鍵管理センタにおいて、配信用公開鍵登録部 2 4 5 がDVD再生機器 2 2 0 用に生成された配信用公開鍵を配信用公開鍵データベース 2 4 7 に登録する（ステップS 4 8）。

【0 0 8 3】（9）機器メーカーにおいて、ICカード記録部 2 1 4 が送出部 2 4 4 から送出されたDVD再生機器 2 2 0 用のデジタル署名付き暗号化秘密鍵を入手してICカード 2 3 0 に記録して、DVD再生機器 2 2 0 と共に出荷する（ステップS 4 9）。図 8 は、DVDディスク製造時の手順を示す図である。

【0 0 8 4】以下に、図 8 を用いてDVDディスク製造時の手順を説明する。

（1）コンテンツメーカーにおいて、コンテンツ鍵管理部 3 5 1 が、現時点において有効なコンテンツ鍵をディスク制作装置 3 6 0 へ供給し、コンテンツ管理部 3 5 2 が、供給すべきコンテンツをディスク制作装置 3 6 0 へ供給する（ステップS 5 1）。

【0 0 8 5】（2）ディスク制作者において、コンテンツ鍵受渡し部 3 6 1 が、コンテンツ鍵管理部 3 5 1 よりコンテンツ鍵の供給を受け、コンテンツ鍵暗号化部 3 4 1 に渡す（ステップS 5 2）。

（3）鍵管理センタにおいて、コンテンツ鍵暗号化部 3 4 1 が、コンテンツ鍵受渡し部 3 6 1 からコンテンツ鍵を受け取り、当該コンテンツ鍵を、配信用公開鍵データベース 2 4 7 に記録された現時点において有効な全てのDVD再生機器用の配信用公開鍵をそれぞれ用いて暗号化して、それぞれのDVD再生機器用の暗号化コンテンツ鍵を生成して、暗号化コンテンツ鍵受渡し部 3 6 3 に渡す（ステップS 5 3）。

【0 0 8 6】（4）ディスク制作者において、暗号化コンテンツ鍵受渡し部 3 6 3 が、コンテンツ鍵暗号化部 3 4 1 から、それぞれのDVD再生機器用の暗号化コンテンツ鍵の供給を受け、制作部 3 6 4 へ渡す（ステップS 5 4）。

（5）ディスク制作者において、コンテンツ暗号化部 3 6 2 が、コンテンツ管理部 3 5 2 よりコンテンツの供給を受け、コンテンツ鍵受渡し部 3 6 1 からコンテンツ鍵の供給を受け、当該コンテンツを当該コンテンツ鍵を用いて暗号化して暗号化コンテンツを生成して制作部 3 6 4 へ渡す（ステップS 5 5）。

【0 0 8 7】（6）ディスク制作者において、制作部 3 6 4 が、コンテンツ暗号化部 3 6 2 から渡された暗号化コンテンツと、暗号化コンテンツ鍵受渡し部 3 6 3 から渡されたそれぞれのDVD再生機器用の暗号化コンテンツ鍵とを記録したDVDディスク 3 7 0 を制作する（ステップS 5 6）。図 9 は、DVDディスク再生時の手順を示す図である。

【0 0 8 8】以下に、図 9 を用いてDVDディスク再生時の手順を説明する。

（1）DVD再生機器 2 2 0 において、ICカードスロットにICカード 2 3 0 又はICカード 3 3 0 を挿入し、所定位置にDVDディスク 3 7 0 をセットする（ステップS 6 1）。

（2）秘密鍵復号部 3 2 1 が、ICカードスロットに挿入されたICカード 2 3 0 又はICカード 3 3 0 から暗号化秘密鍵を読み出し、当該暗号化秘密鍵に施されたデジタル署名に基づいて、当該暗号化秘密鍵が正当なものであるか否かを判断する（ステップS 6 2）。当該暗号化秘密鍵が正当なものであると判断されなかった場合には、DVDディスクの再生をせずに処理を終了する。

【0 0 8 9】（3）暗号化秘密鍵が正当なものであると判断された場合には、秘密鍵復号部 3 2 1 が、当該暗号化秘密鍵を、秘密鍵記録部 2 2 1 に記録されている初期秘密鍵を用いて復号して配信用秘密鍵を生成する（ステップS 6 3）。

（4）コンテンツ鍵復号部 3 2 2 が、DVDディスク 3 7 0 に記録されたDVD再生機器 2 2 0 用の暗号化コンテンツ鍵を、秘密鍵復号部 3 2 1 により生成された配信用秘密鍵を用いて復号してコンテンツ鍵を生成する（ステップS 6 4）。

【0 0 9 0】（5）コンテンツ復号部 3 2 3 が、DVDディスク 3 7 0 に記録された暗号化コンテンツを、コンテンツ鍵復号部 3 2 2 により生成されたコンテンツ鍵を用いて復号してコンテンツを得る（ステップS 6 5）。図 1 0 は、ICカード更新時の手順を示す図である。以下に、図 1 0 を用いてICカード更新時の手順を説明する。

【0 0 9 1】（1）鍵管理センタにおいて、認知部 3 4 2 が、DVD再生機器毎に不正なく正常に稼動しているかを監視し、DVDディスクの再生を禁止すべきDVD再生機器や、配信用秘密鍵を更新すべきDVD再生機器を認知する。ここではDVD再生機器 2 2 0 の配信用秘密鍵を更新すべきであると認知したものとする（ステップS 7 1）。

【0 0 9 2】（2）鍵管理センタにおいて、配信用鍵生成部 2 4 2 が、DVD再生機器 2 2 0 用に、配信用公開鍵、及び、配信用秘密鍵を生成する（ステップS 7 2）。

（3）鍵管理センタにおいて、秘密鍵暗号化部 2 4 3 が、DVD再生機器 2 2 0 用に生成された配信用秘密鍵を、初期公開鍵データベース 2 4 6 に登録されているDVD再生機器 2 2 0 用の初期公開鍵を用いて暗号化して暗号化秘密鍵を生成し、さらに、デジタル署名を施す（ステップS 7 3）。

【0 0 9 3】（4）鍵管理センタにおいて、新ICカード作成部 3 4 4 が、DVD再生機器 2 2 0 用の暗号化秘密鍵を、新しいICカードに記録してICカード 3 3 0 を作成し、当該DVD再生機器へ向けて送出する（ステップS 7 4）。

(5) DVD再生機器220において、ICカード更新部324が、新ICカード作成部344からICカード330を受付けた後は、DVD再生機器220のICカードスロットにICカード330を挿入して、以後のDVDディスクの再生に備える(ステップS75)。

【0094】なお、鍵管理センタ装置とディスク制作装置とは同一の装置であってもよい。以上のように、本発明の実施の形態2によれば、鍵管理センタが主導的に、配信用の鍵ペアを更新することができる。なお、本発明の実施の形態1及び2によれば、公開鍵暗号方式としてElGamal暗号方式を用いるものとしているが、他の公開鍵暗号方式であっても構わない。

【0095】また、本発明の実施の形態1及び2によれば、鍵管理センタにより供給される暗号化秘密鍵の正当性を証明するために、ElGamal暗号方式を用いた署名方式を用いるものとしているが、この方式に限られるものではなく、暗号化秘密鍵の正当性を証明することができる方式であれば何であっても構わない。また、本発明の実施の形態1及び2において、暗号化秘密鍵、暗号化コンテンツ鍵、暗号化コンテンツ等を配信する手段は、通信路介した伝送であってもよいし、例えばフレキシブルディスク、CD、MO、DVD、メモ리카ード等の着脱可能な可搬記録媒体による配送であってもよく、暗号化コンテンツを配信できるのであれば何であっても構わない。

【0096】また、本発明の実施の形態1及び2において、鍵管理センタは複数であってもよく、各鍵管理センタはそれぞれ独立に暗号鍵を管理し、各受信端末又はDVD再生機器は各鍵管理センタ毎に暗号鍵を管理してもよい。

【0097】

【発明の効果】本発明に係る更新方法は、鍵管理センタと配信局と1つ以上の受信端末とを含むデータ配信システムにおいて公開鍵暗号方式の鍵ペアをなす配信用公開鍵及び配信用秘密鍵を更新する更新方法であって、配信用公開鍵は配信すべきデータを暗号化して暗号化データを生成する際に用いられ、配信用秘密鍵は配信された暗号化データを復号する際に用いられ、当該更新方法は、所定の受信端末においてデータ配信を始める前に更新用秘密鍵を入手する秘密鍵入手ステップと、前記鍵管理センタにおいてデータ配信を始める前に前記更新用秘密鍵と鍵ペアをなす更新用公開鍵を入手する公開鍵入手ステップと、前記鍵管理センタにおいて前記受信端末用に配信用公開鍵及び配信用秘密鍵を生成する生成ステップと、前記鍵管理センタにおいて前記生成ステップにより生成された配信用秘密鍵を前記公開鍵入手ステップにより入手された更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成する暗号化ステップと、前記鍵管理センタにおいて任意のタイミングで前記暗号化ステップにより生成された暗号化秘密鍵を前記受信端末へ向けて送出する

送出ステップと、前記鍵管理センタにおいて前記送出ステップにより暗号化秘密鍵が前記受信端末へ向けて送出された後はデータ配信の際に配信局により使用される当該受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成手段により当該受信端末用に生成された配信用公開鍵に更新する公開鍵更新ステップと、前記受信端末において前記送出ステップにより送出された暗号化秘密鍵を受付ける受け付けステップと、前記受信端末において前記受け付けステップにより暗号化秘密鍵が受け付けられた後は当該受信端末用の配信用秘密鍵をそれまで使用していた配信用秘密鍵から前記秘密鍵入手ステップにより入手された更新用秘密鍵を用いて当該暗号化秘密鍵を必要に応じて復号することにより復元される配信用秘密鍵に更新する秘密鍵更新ステップとを含むことを特徴とする。

【0098】これによって、鍵管理センタが配信用公開鍵、及び、配信用秘密鍵を生成し、配信用秘密鍵を更新用公開鍵を用いて暗号化して送出することができる。従って、鍵配送時の安全性を損なわずに、鍵管理センタが配信用鍵ペアの更新の主導権を持つことができる。また、更新方法において、前記暗号化ステップは、さらに、生成する暗号化秘密鍵に当該暗号化秘密鍵の正当性を示すデジタル署名を施し、前記秘密鍵更新ステップは、前記受け付けステップにより受け付けられた暗号化秘密鍵に施されたデジタル署名に基づいて当該暗号化秘密鍵が正当なものであるか否かを判断し正当なものであると判断した場合に配信用秘密鍵を更新し正当なものではないと判断した場合に配信用秘密鍵を更新しないことを特徴とすることもできる。

【0099】これによって、暗号化秘密鍵にデジタル署名を施し、受け付けられた暗号化秘密鍵が正当なものであるか否かを判断することができる。従って、正当でない配信用鍵で誤って、配信用秘密鍵を更新することを防止できる。また、更新方法において、前記受信端末は複数であり、それぞれの受信端末用の配信用公開鍵は配信すべきデータをそれぞれ暗号化して暗号化データを生成する際に用いられ、それぞれの受信端末用の配信用秘密鍵は対応する受信端末において配信された暗号化データを復号する際に用いられ、前記秘密鍵入手ステップはそれぞれの受信端末においてそれぞれユニークな更新用秘密鍵を入手し、前記公開鍵入手ステップは前記鍵管理センタにおいてそれぞれの受信端末用のそれぞれユニークな更新用公開鍵を入手し、前記生成ステップは、前記鍵管理センタにおいてそれぞれの受信端末用にそれぞれユニークな配信用公開鍵及び配信用秘密鍵を生成し、前記暗号化ステップは、前記鍵管理センタにおいて前記生成ステップによりそれぞれの受信端末用に生成された配信用秘密鍵をそれぞれの受信端末用の更新用公開鍵を用いて暗号化してそれぞれの受信端末用の暗号化秘密鍵を生成し、前記送出ステップは、前記鍵管理センタにおいて任

意のタイミングで一斉に前記暗号化ステップにより生成されたそれぞれの受信端末用の暗号化秘密鍵をそれぞれの受信端末へ向けて送出し、前記公開鍵更新ステップは、前記鍵管理センタにおいて前記送出ステップによりそれぞれの受信端末用の暗号化秘密鍵がそれぞれの受信端末へ向けて一斉に送出された後はデータ配信の際に配信局により使用されるそれぞれの受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成ステップによりそれぞれの受信端末用に生成された配信用公開鍵に更新し、前記受付けステップは、それぞれの受信端末において前記送出ステップにより送出されたそれぞれの受信端末用の暗号化秘密鍵を受付け、前記秘密鍵更新ステップは、それぞれの受信端末において前記受付けステップによりそれぞれの受信端末用の暗号化秘密鍵が受付けられた後はそれぞれの受信端末用の配信用秘密鍵をそれまで使用していた配信用秘密鍵から秘密鍵入手ステップにより入手されたそれぞれの更新用秘密鍵を用いて当該暗号化秘密鍵を必要に応じて復号することにより復元される配信用秘密鍵に更新することを特徴とすることもできる。

【0100】これによって、配信用の鍵ペアの更新を一斉におこなうことができる。また、更新方法において、当該更新方法は、さらに、前記配信局においてデータ配信を中止すべき受信端末を認知する認知ステップと、前記配信局において前記認知ステップによりデータ配信を中止すべき受信端末が認知された以後は当該受信端末用の暗号化データの配信を禁止する配信禁止ステップとを含むことを特徴とすることもできる。

【0101】これによって、鍵管理センタが主導的に、一部の受信端末だけ暗号化データの配信を禁止することができる。また、更新方法において、当該更新方法は、さらに、前記鍵管理センタにおいて配信用秘密鍵を更新すべき受信端末を認知する認知ステップを含み、前記生成ステップは、前記鍵管理センタにおいて前記認知ステップにより認知された受信端末用の配信用公開鍵及び配信用秘密鍵を生成し、前記暗号化ステップは、前記鍵管理センタにおいて前記認知ステップにより認知された受信端末用に前記生成ステップにより生成された配信用秘密鍵を当該受信端末用の更新用公開鍵を用いて暗号化して当該受信端末用の暗号化秘密鍵を生成し、前記送出ステップは、前記鍵管理センタにおいて前記認知ステップにより認知された受信端末用に前記暗号化ステップにより生成された暗号化秘密鍵を当該受信端末へ向けて送出し、前記公開鍵更新ステップは、前記鍵管理センタにおいて前記認知ステップにより認知された受信端末へ向けて暗号化秘密鍵が送出された後はデータ配信の際に配信局により使用される当該受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成ステップにより当該受信端末用に生成された配信用公開鍵に更新し、前記秘密鍵更新ステップは、前記認知ステップに

より認知された受信端末において当該受信端末用の暗号化秘密鍵が受付けられた後は当該受信端末用の配信用秘密鍵をそれまで使用していた配信用秘密鍵から秘密鍵入手ステップにより入手された更新用秘密鍵を用いて必要に応じて復号することにより復元される配信用秘密鍵に更新することを特徴とすることもできる。

【0102】これによって、鍵管理センタが主導的に、一部の受信端末だけの配信用秘密鍵を更新することができる。また、更新方法において、それぞれの受信端末用の配信用公開鍵を用いてそれぞれ暗号化される配信すべきデータは秘密鍵暗号方式の鍵であるコンテンツ鍵であり、前記配信局はそれぞれの受信端末用の配信用公開鍵を用いて前記コンテンツ鍵を暗号化してそれぞれの受信端末用の暗号化コンテンツ鍵を生成し配信すべきコンテンツを前記コンテンツ鍵を用いて暗号化して暗号化コンテンツを生成し前記それぞれの受信端末用の暗号化コンテンツ鍵の全てと前記暗号化コンテンツとを全ての受信端末へ配信し、前記それぞれの受信端末は前記配信局より配信された全ての暗号化コンテンツ鍵と暗号化コンテンツとを受信し当該受信端末用の暗号化コンテンツ鍵を当該受信端末用の配信用秘密鍵を用いて復号して前記コンテンツ鍵を復元し前記暗号化コンテンツを当該コンテンツ鍵を用いて復号してコンテンツを復元することを特徴とすることもできる。

【0103】これによって、配信局から全ての受信端末用へ、配信すべきコンテンツをコンテンツ鍵を用いて暗号化した暗号化コンテンツと、コンテンツ鍵を各受信端末用の配信用秘密鍵を用いて暗号化した各受信端末用の暗号化コンテンツ鍵の全てとが配信されるので、配信データの総量が押さえられ、またコンテンツの復号に係る各装置の負荷が軽減される。

【0104】また、更新方法において、前記受信端末は当該受信端末用の暗号化秘密鍵を記録したＩＣカードを備え、当該暗号化秘密鍵を復号して配信用秘密鍵を生成し、受信した暗号化データを、当該配信用秘密鍵を用いて復号し、前記送出ステップは、前記鍵管理センタにおいて前記暗号化ステップにより生成された前記受信端末用の暗号化秘密鍵を新しいＩＣカードに記録して当該受信端末へ向けて送出し、前記受付けステップは、前記受信端末において前記新しいＩＣカードを受付け、前記秘密鍵更新ステップは、前記受信端末において前記新しいＩＣカードが受付けられた後に元々備えていたＩＣカードが当該新しいＩＣカードと差し換えられることにより配信用秘密鍵が更新されることを特徴とすることもできる。

【0105】これによって、新しい暗号化秘密鍵を新しいＩＣカードに記録して、ＩＣカードを差し換えることにより配信用秘密鍵を更新するので、新しい暗号化秘密鍵を公衆回線等を用いて伝達するよりも、より安全性が高い。本発明に係る受信端末は、所定データが当該受信

端末用の配信用公開鍵を用いて暗号化されることにより生成された配信局から配信される暗号化データを受信して当該暗号化データを当該受信端末用の配信用秘密鍵を用いて復号して前記所定データを得る受信端末であって、データ配信を始める前に更新用秘密鍵を入手する秘密鍵入手手段と、当該受信端末用の配信用秘密鍵が前記更新用秘密鍵と鍵ペアをなす更新用公開鍵を用いて暗号化されることにより生成された暗号化秘密鍵を保持する保持手段と、前記配信局より配信される前記暗号化データを受信する受信手段と、前記保持手段に保持されている暗号化秘密鍵を前記秘密鍵入手手段により入手された更新用秘密鍵を用いて復号して当該受信端末用の配信用秘密鍵を復元する秘密鍵復号手段と、前記受信手段により受信された暗号化データを前記秘密鍵復号手段により復元された配信用秘密鍵を用いて復号して前記所定データを得るデータ復号手段とを備えることを特徴とする。

【0106】これによって、保持している暗号化秘密鍵を、入手された源秘密鍵を用いて復号して配信用秘密鍵を生成し、受信した暗号化データを、生成した配信用秘密鍵を用いて復号して、前記所定データを得ることができる。従って、源秘密鍵を各受信端末において秘密に入手することができさえすれば、配信用秘密鍵を受信端末以外が容易に更新することができるので、鍵配送時の安全性を損なわずに、受信端末以外に配信用鍵ペアの更新の主導権を持たせることができる。

【0107】また、受信端末において、当該受信端末は、さらに、鍵管理センタから任意のタイミングで送出される暗号化秘密鍵を受付ける受け付け手段を備え、前記暗号化秘密鍵は前記鍵管理センタにおいて当該受信端末用に公開鍵暗号方式の鍵ペアをなす配信用公開鍵及び配信用秘密鍵が生成され前記更新用公開鍵を用いて当該配信用秘密鍵が暗号化されて生成され、当該受信端末は、さらに、前記受け付け手段により暗号化秘密鍵が受け付けられた後は前記保持手段に保持された暗号化秘密鍵を当該受け付けられた暗号化秘密鍵に更新する秘密鍵更新手段を備えることを特徴とすることもできる。

【0108】これによって、鍵管理センタにより配信用公開鍵、及び、配信用秘密鍵が生成され、鍵管理センタにより生成された配信用秘密鍵が更新用公開鍵を用いて暗号化されて生成された新しい暗号化秘密鍵が送出されるので、当該新しい暗号化秘密鍵を受付けて、保持手段に保持された暗号化秘密鍵を当該新しい暗号化秘密鍵で更新することができる。

【0109】したがって、鍵配送時の安全性を損なわずに、鍵管理センタに配信用鍵ペアの更新の主導権を持たせることができる。また、受信端末において、前記受け付け手段により受け付けられる暗号化秘密鍵には当該暗号化秘密鍵の正当性を示すデジタル署名が施されており、前記秘密鍵復号手段は、前記秘密鍵更新手段により暗号化秘密鍵が更新された後は更新された暗号化秘密鍵に施さ

れたデジタル署名に基づいて当該暗号化秘密鍵が正当なものであるか否かを判断し正当なものであると判断した場合に当該受信端末用の配信用秘密鍵を復元し正当なものではないと判断した場合に当該受信端末用の配信用秘密鍵を復元しないことを特徴とすることもできる。

【0110】これによって、保持されている暗号化秘密鍵にはデジタル署名が施されているので、暗号化秘密鍵が正当なものであるか否かを判断することができる。従って、正当でない配信用秘密鍵を誤って使用することを防止できる。また、受信端末において、前記所定データは秘密鍵暗号方式の鍵であるコンテンツ鍵であり、前記受信手段は、前記配信用公開鍵を用いて前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵と共に当該コンテンツ鍵を用いて配信すべきコンテンツを暗号化して生成された暗号化コンテンツを受信し、前記データ復号手段は、前記受信手段により受信された暗号化コンテンツ鍵を前記秘密鍵復号手段により復元された配信用秘密鍵を用いて復号して前記コンテンツ鍵を得て前記受信手段により受信された暗号化コンテンツを当該コンテンツ鍵を用いて復号してコンテンツを得ることを特徴とすることもできる。

【0111】これによって、配信局から全ての受信端末へ、配信すべきコンテンツがコンテンツ鍵を用いて暗号化された暗号化コンテンツと、コンテンツ鍵が各受信端末用の配信用秘密鍵を用いて暗号化された各受信端末用の暗号化コンテンツ鍵の全てとが配信されるので、配信データの総量が押さえられ、またコンテンツの復号に係る各装置の負荷が軽減される。

【0112】また、受信端末において、前記保持手段はＩＣカードであり、前記受け付け手段は、前記暗号化秘密鍵が記録された新しいＩＣカードを受け付け、前記秘密鍵更新手段は、前記新しいＩＣカードが受け付けられた後は元々備えていたＩＣカードが当該新しいＩＣカードと差し換えられることにより配信用秘密鍵が更新されることを特徴とすることもできる。

【0113】これによって、新しい暗号化秘密鍵が記録された新しいＩＣカードを、元々備えていたＩＣカードと差し換えることにより配信用秘密鍵を更新するので、新しい暗号化秘密鍵を公衆回線等を用いて伝達するよりも、より安全性が高い。本発明に係る鍵管理装置は、データ配信を始める前に更新用秘密鍵を保持している所定の受信端末用に当該更新用秘密鍵と鍵ペアをなす更新用公開鍵を入手する公開鍵入手手段と、前記受信端末用に公開鍵暗号方式の鍵ペアをなす配信用公開鍵及び配信用秘密鍵を生成する生成手段と、前記生成手段により生成された配信用秘密鍵を前記公開鍵入手手段により入手された更新用公開鍵を用いて暗号化して暗号化秘密鍵を生成する暗号化手段と、任意のタイミングで前記暗号化手段により生成された暗号化秘密鍵を前記受信端末へ向けて送出する送出手段と、前記送出手段により暗号化秘密

鍵が前記受信端末へ向けて送出された後はデータ配信の際に使用される当該受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成手段により当該受信端末用に生成された配信用公開鍵に更新する公開鍵更新手段とを備えることを特徴とする。

【0114】これによって、鍵管理装置が配信用公開鍵、及び、配信用秘密鍵を生成し、配信用秘密鍵を更新用公開鍵を用いて暗号化して送出することができる。従って、鍵配送時の安全性を損なわずに、鍵管理装置が配信用鍵ペアの更新の主導権を持つことができる。また、鍵管理装置において、前記暗号化手段は、さらに、生成する暗号化秘密鍵に当該暗号化秘密鍵の正当性を示すデジタル署名を施すことを特徴とすることもできる。

【0115】これによって、暗号化秘密鍵にデジタル署名を施すので、受信端末において受け取られた暗号化秘密鍵が正当なものであるか否かを判断することができる。従って、受信端末において正当でない配信用秘密鍵に誤って更新されることが防止できる。また、鍵管理装置において、前記公開鍵入手手段は複数の受信端末用のそれぞれユニークな更新用公開鍵を入手し、前記生成手段は、それぞれの受信端末用にそれぞれユニークな配信用公開鍵及び配信用秘密鍵を生成し、前記暗号化手段は、前記生成手段によりそれぞれの受信端末用に生成された配信用秘密鍵をそれぞれの受信端末用の更新用公開鍵を用いて暗号化してそれぞれの受信端末用の暗号化秘密鍵を生成し、前記送出手段は、任意のタイミングで一斉に前記暗号化手段により生成されたそれぞれの受信端末用の暗号化秘密鍵をそれぞれ対応する受信端末へ向けて送出し、前記公開鍵更新手段は、前記送出手段によりそれぞれの受信端末用の暗号化秘密鍵がそれぞれ対応する受信端末へ向けて一斉に送出された後はそれぞれの受信端末用の配信用公開鍵をそれまで使用していた配信用公開鍵から前記生成手段によりそれぞれの受信端末用に生成された配信用公開鍵に更新することを特徴とすることもできる。

【0116】これによって、配信用の鍵ペアの更新を一斉におこなうことができる。また、鍵管理装置において、当該鍵管理装置は、さらに、データ配信を中止すべき受信端末を認知する認知手段と、前記認知手段によりデータ配信を中止すべき受信端末が認知された以後は当該受信端末用の配信用公開鍵を用いたデータ配信を禁止する配信禁止手段とを備えることを特徴とすることもできる。

【0117】これによって、鍵管理装置が主導的に、一部の受信端末だけ暗号化データの配信を禁止することができる。また、鍵管理装置において、当該鍵管理装置は、さらに、配信用秘密鍵を更新すべき受信端末を認知する認知手段を備え、前記生成手段は、前記認知手段により認知された受信端末用の配信用公開鍵及び配信用秘密鍵を生成し、前記暗号化手段は、前記認知手段により

認知された受信端末用に前記生成手段により生成された配信用秘密鍵を当該受信端末用の更新用公開鍵を用いて暗号化して当該受信端末用の暗号化秘密鍵を生成し、前記送出手段は、前記認知手段により認知された受信端末用に前記暗号化手段により生成された暗号化秘密鍵を当該受信端末へ向けて送出し、前記公開鍵更新手段は、前記認知手段により認知された受信端末へ向けて暗号化秘密鍵が送出された後は当該受信端末用の配信用公開鍵をそれまで使用されていた配信用公開鍵から前記生成手段により当該受信端末用に生成された配信用公開鍵に更新することを特徴とすることもできる。

【0118】これによって、鍵管理装置が主導的に、一部の受信端末だけの配信用秘密鍵を更新することができる。また、鍵管理装置において、当該鍵管理装置は配信局と一体化しており、当該鍵管理装置は、さらに、所定データをそれぞれの受信端末用の配信用公開鍵を用いて暗号化してそれぞれの受信端末用の暗号化データを生成する配信データ生成手段と、前記配信データ生成手段により生成されたそれぞれの受信端末用の暗号化データの全てを全ての受信端末へ配信する配信手段とを備えることを特徴とすることもできる。

【0119】これによって、配信局が配信用の鍵ペアの更新を一斉におこなうことができる。また、鍵管理装置において、前記所定データは秘密鍵暗号方式の鍵であるコンテンツ鍵であり、前記配信データ生成手段は、コンテンツ鍵をそれぞれの受信端末用の配信用公開鍵を用いて暗号化してそれぞれの受信端末用の暗号化コンテンツ鍵を生成すると共に当該コンテンツ鍵を用いて配信すべきコンテンツを暗号化して暗号化コンテンツを生成し、前記配信手段は、前記それぞれの受信端末用の暗号化コンテンツ鍵の全てと共に前記配信データ生成手段により生成された前記暗号化コンテンツを全ての受信端末へ配信することを特徴とすることもできる。

【0120】これによって、配信局から全ての受信端末用へ、配信すべきコンテンツをコンテンツ鍵を用いて暗号化した暗号化コンテンツと、コンテンツ鍵を各受信端末用の配信用秘密鍵を用いて暗号化した各受信端末用の暗号化コンテンツ鍵の全てとを配信するので、配信データの総量が押さえられ、またコンテンツの復号に係る各装置の負荷が軽減される。

【0121】また、鍵管理装置において、前記受信端末は当該受信端末用の暗号化秘密鍵を記録したＩＣカードを備えデータ配信の際に当該暗号化秘密鍵を復号して配信用秘密鍵を生成して用い、前記送出手段は、前記暗号化手段により生成された前記受信端末用の暗号化秘密鍵を新しいＩＣカードに記録して当該受信端末へ送ることを特徴とすることもできる。これによって、新しい暗号化秘密鍵を新しいＩＣカードに記録して、各受信端末へ送り、各受信端末においてはＩＣカードを差し換えることにより配信用秘密鍵を更新するので、新しい暗号化

秘密鍵を公衆回線等を用いて伝達するよりも、より安全性が高い。

【図面の簡単な説明】

【図１】本発明の実施の形態１の配信システムを示す図である。

【図２】コンテンツの配信を始める前に予め行う準備の手順を示す図である。

【図３】コンテンツの配信時の手順を示す図である。

【図４】鍵更新時の手順を示す図である。

【図５】本発明の実施の形態２のＤＶＤ再生機器の製造システムを示す図である。

【図６】本発明の実施の形態２の配信システムを示す図である。

【図７】ＤＶＤ再生機器の製造時の手順を示す図である。

【図８】ＤＶＤディスク製造時の手順を示す図である。

【図９】ＤＶＤディスク再生時の手順を示す図である。

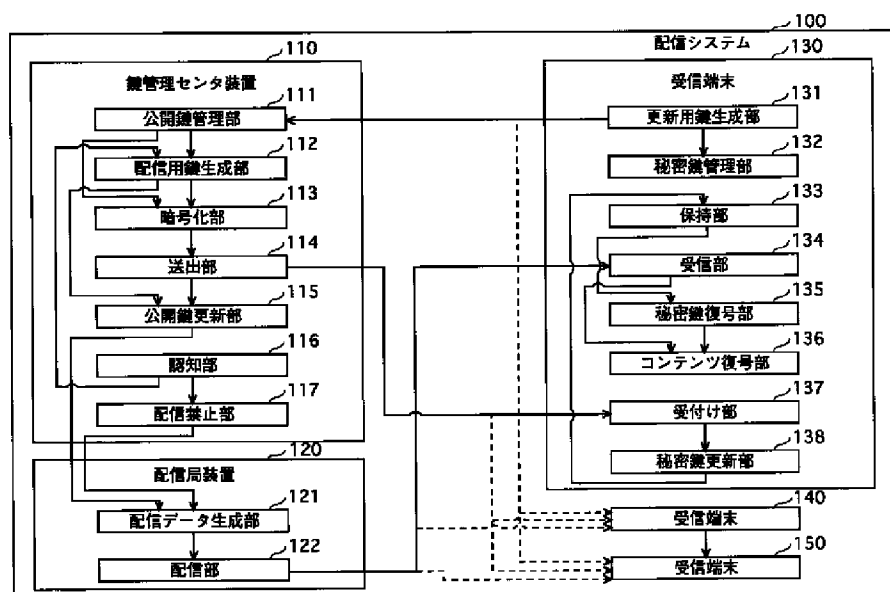
【図１０】ＩＣカード更新時の手順を示す図である。

【符号の説明】

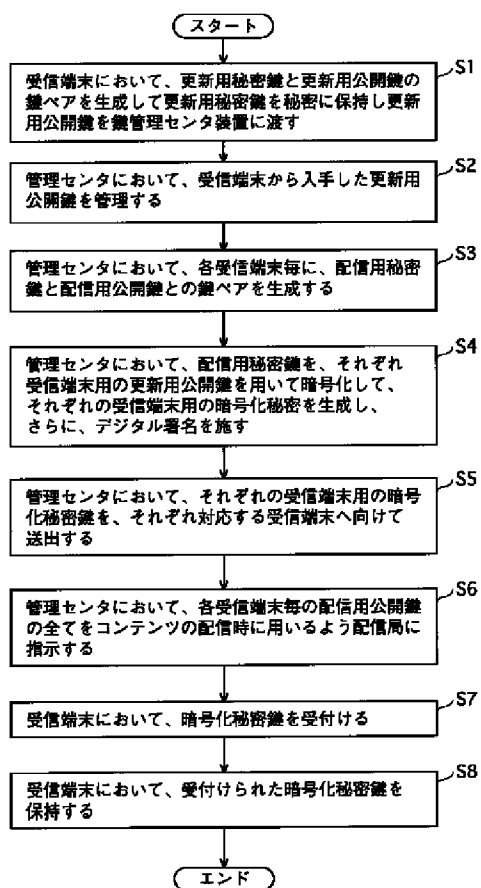
１００ 配信システム  
１１０ 鍵管理センタ装置  
１１１ 公開鍵管理部  
１１２ 配信用鍵生成部  
１１３ 暗号化部  
１１４ 送出部  
１１５ 公開鍵更新部  
１１６ 認知部  
１１７ 配信禁止部  
１２０ 配信局装置  
１２１ 配信データ生成部  
１２２ 配信部  
１３０ 受信端末  
１３１ 更新用鍵生成部  
１３２ 秘密鍵管理部  
１３３ 保持部  
１３４ 受信部  
１３５ 秘密鍵復号部  
１３６ コンテンツ復号部  
１３７ 受付け部

１３８ 秘密鍵更新部  
１４０ 受信端末  
１５０ 受信端末  
２００ 製造システム  
２１０ 機器メーカ装置  
２１１ 初期鍵生成部  
２１２ 鍵書込み部  
２１３ 公開鍵伝送部  
２１４ ＩＣカード記録部  
２２０ ＤＶＤ再生機器  
２２１ 秘密鍵記録部  
２３０ ＩＣカード  
２４０ 鍵管理センタ装置  
２４１ 初期公開鍵登録部  
２４２ 配信用鍵生成部  
２４３ 秘密鍵暗号化部  
２４４ 送出部  
２４５ 配信用公開鍵登録部  
２４６ 初期公開鍵データベース  
２４７ 配信用公開鍵データベース  
３００ 配信システム  
３２１ 秘密鍵復号部  
３２２ コンテンツ鍵復号部  
３２３ コンテンツ復号部  
３２４ ＩＣカード更新部  
３３０ ＩＣカード  
３４１ コンテンツ鍵暗号化部  
３４２ 認知部  
３４３ 登録抹消部  
３４４ 新ＩＣカード作成部  
３５０ コンテンツメーカ装置  
３５１ コンテンツ鍵管理部  
３５２ コンテンツ管理部  
３６０ ディスク制作装置  
３６１ コンテンツ鍵受渡し部  
３６２ コンテンツ暗号化部  
３６３ 暗号化コンテンツ鍵受渡し部  
３６４ 制作部  
３７０ ＤＶＤディスク

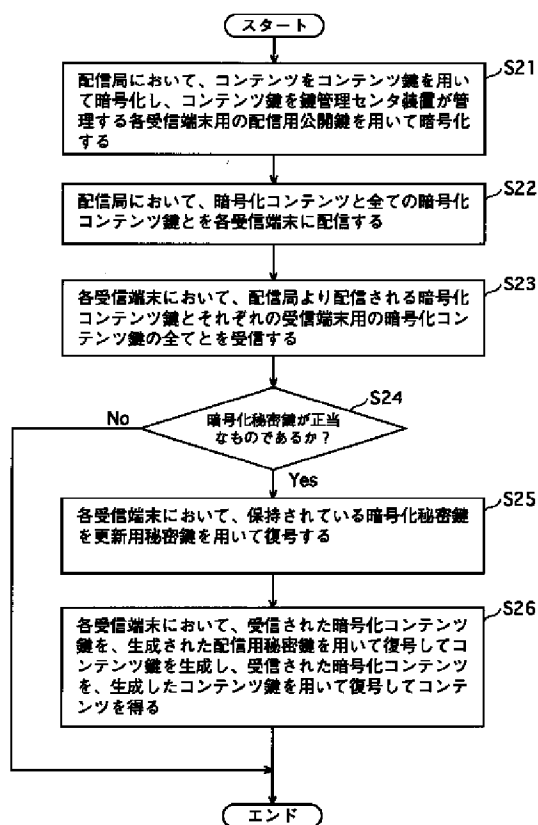
【図1】



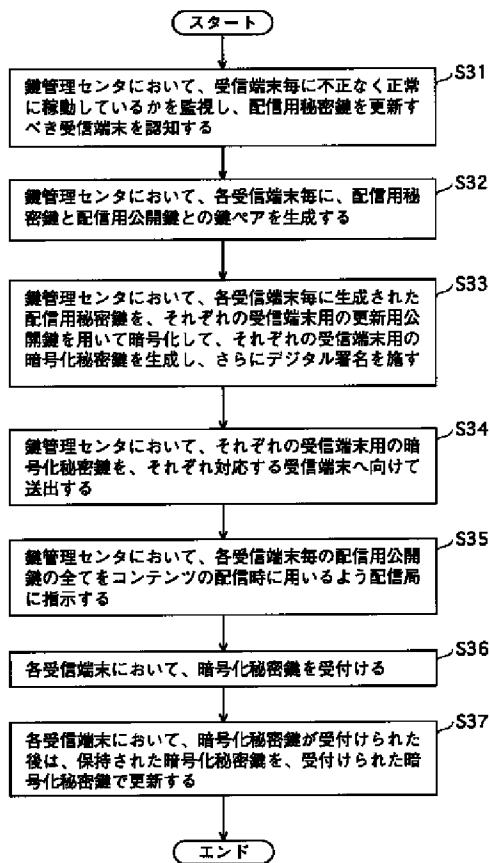
【図2】



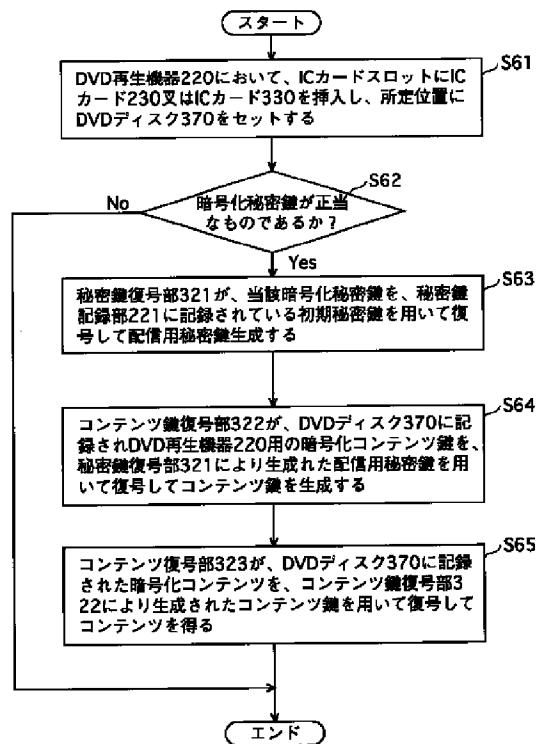
【図3】



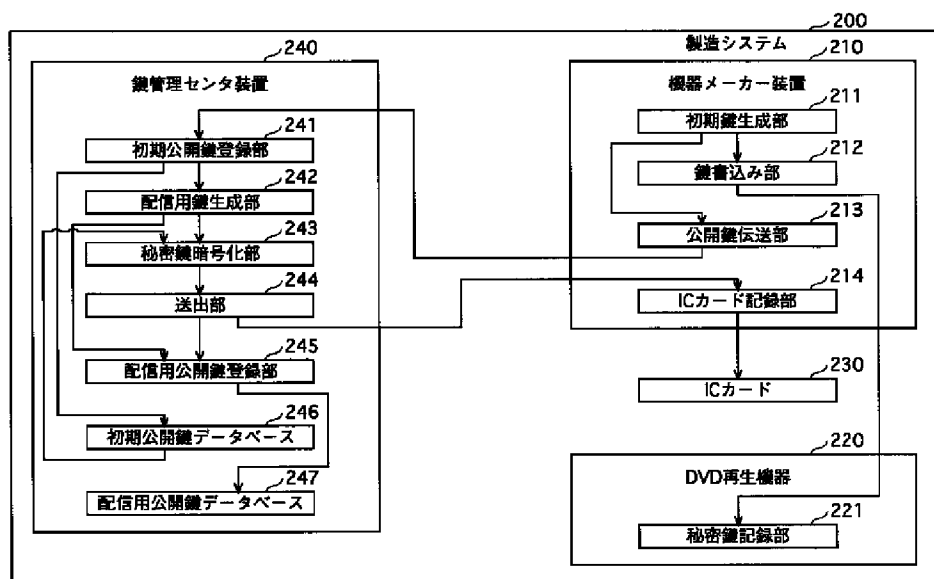
【図4】



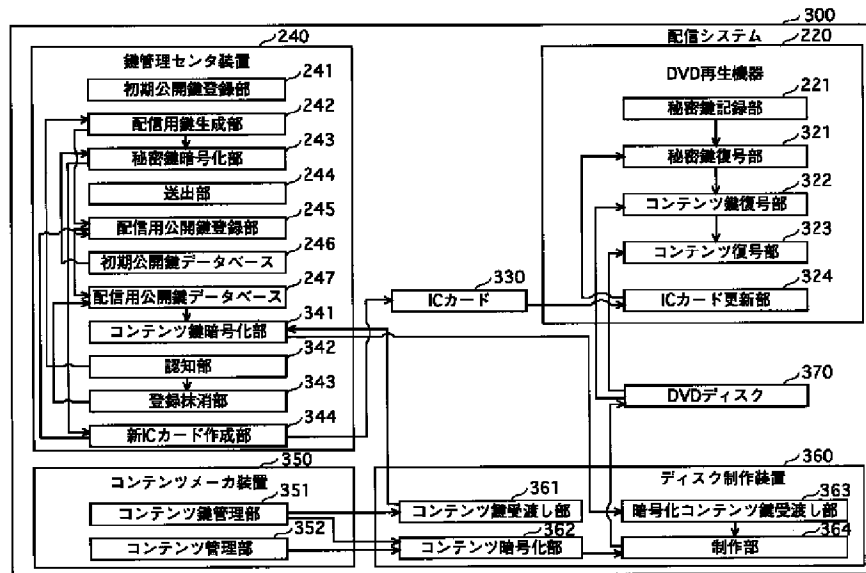
【図9】



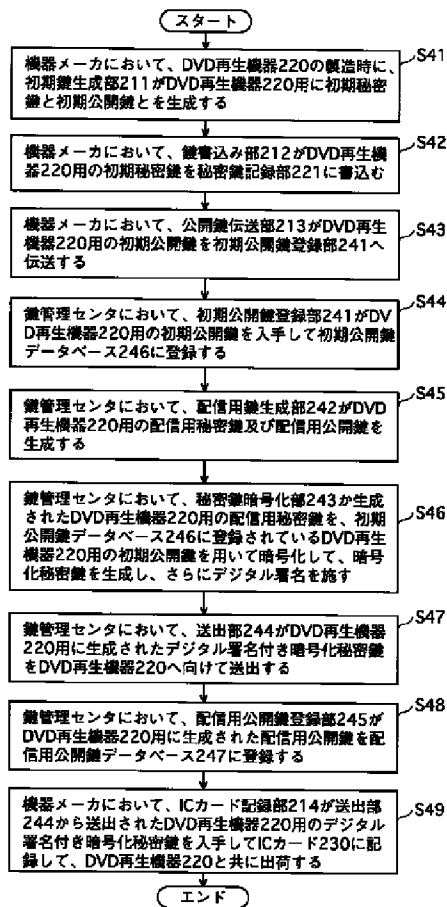
【図5】



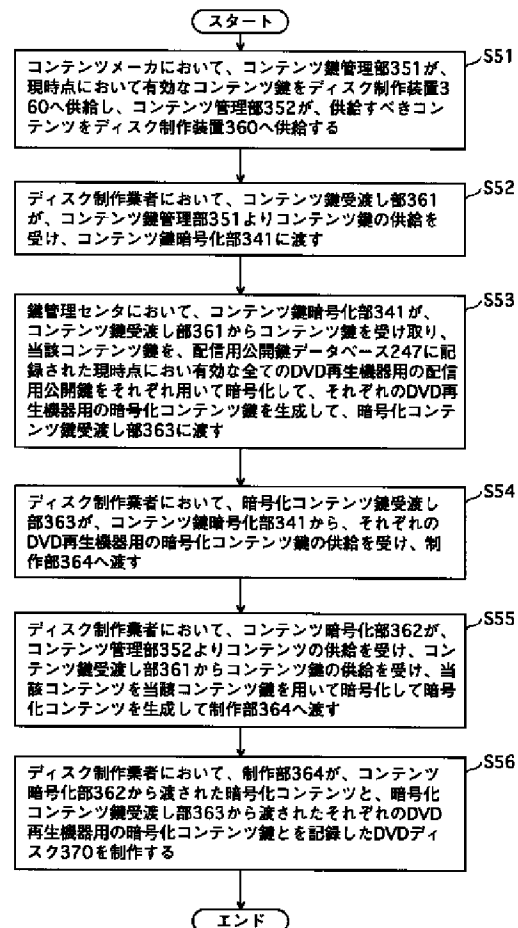
【図6】



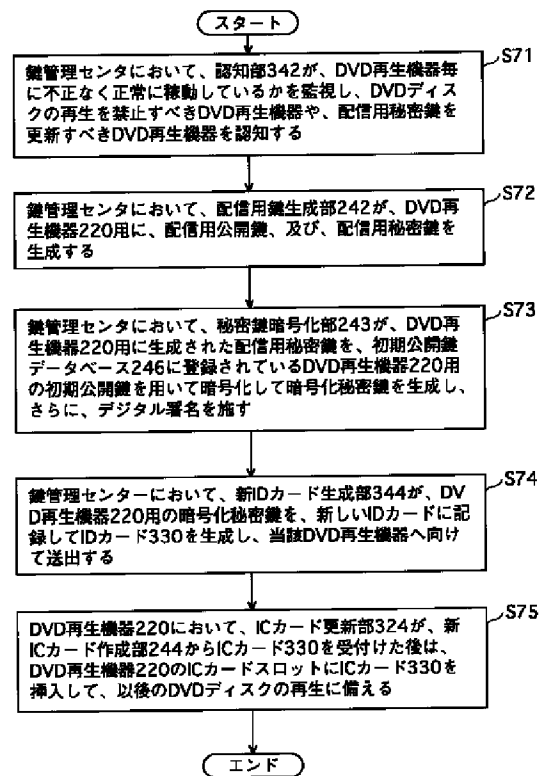
【図7】



【図8】



【図10】



フロントページの続き

Fターム(参考) 5B017 AA03 BA07 CA05 CA14  
5B058 CA01 CA27 KA31 KA35 YA20  
5J104 AA16 AA34 DA03 EA01 EA04  
EA19 EA22 JA21 LA06 MA05  
NA02 NA35 NA37